CUANDO GOOGLE ENCONTRÓ A Wikileaks

JULIAN ASSANGE



En junio de 2011 Julian Assange estaba viviendo bajo arresto domiciliario en Norfolk (Inglaterra), en casa de unos amigos. Allí recibió al entonces presidente de Google, Eric Schmidt, que había solicitado encontrarse con él. Schmidt se presentó con otras tres personas y durante horas mantuvo una larga conversación con Assange. Hablaron de los problemas a los que la sociedad tiene que hacer frente y de las soluciones tecnológicas que podía ofrecer la red global. Posteriormente, en 2013, Schmidt y uno de los presentes, Jared Cohen, publicaron un libro fruto de aquella conversación.

Cuando Julian Assange lo leyó constató que la versión que daban desde Google de su encuentro distaba mucho de ser precisa, y decidió escribir su propia versión de la charla, Cuando Google encontró a WikiLeaks: “Fue una reunión muy interesante […] Yo estaba bajo arresto domiciliario. Teníamos en ese momento un conflicto muy importante con el gobierno de Estados Unidos, con Hillary Clinton y el Pentágono por la publicación de los cables diplomáticos de Estados Unidos ese año […] me dijeron que Eric Schmidt, el jefe de Google, quería venir a verme. Dijimos que sí, que sería interesante escuchar a esta empresa tan potente e influyente, para ver lo que quería”. Eric Schmidt y el nexo entre el Departamento de Estado y Google “En ese preciso momento me di cuenta de que era muy posible que Eric Schmidt no fuera únicamente un emisario de Google… La delegación que me visitó era una cuarta parte Google y tres cuartas partes representaban al Departamento de política exterior de Estados Unidos…”

Google te vigila “Google permite a la ASN (Agencia de Seguridad Norteamericana) y al FBI leer los correos electrónicos. Incluso en una aburrida comisaría de policía o en un juzgado, se puede tener acceso a esos correos sin orden judicial”. Google está fuertemente vinculado al Departamento de Estado norteamericano “Pero también la New American Fundation, que es el *think tank* centrista, agresivo y liberal de Washington DC. Eric Schmidt es también su presidente y su principal fundador, al igual que el de Google”.

Julian Assange

Cuando Google encontró a Wikileaks

ePub r1.0
XcUiDi 01-10-2021

Título original: *When Google Met Wikileaks*
Julian Assange, 2014
Traducción: Iván Barbeitos García

Editor digital: XcUiDi
ePub base r2.1

A mi familia, a la que quiero y añoro mucho.

«El cráneo conectado a los auriculares,
los auriculares conectados al iPhone,
el iPhone conectado a Internet,
conectado a Google,
conectado al gobierno»

MIA, «The Message»

MÁS ALLÁ DEL BIEN Y DEL «NO SEAS MALO»[I]

Eric Schmidt es una figura influyente, incluso entre el desfile de poderosos personajes con los que me he tenido que cruzar desde que fundé WikiLeaks. A mediados de mayo de 2011 me encontraba bajo arresto domiciliario en la zona rural de Norfolk, a unas tres horas en coche al nordeste de Londres. Las severas medidas aplicadas contra nuestro trabajo se encontraban en su punto culminante, y cada momento desperdiciado parecía una eternidad, por lo que era realmente difícil conseguir mi atención. Sin embargo, cuando mi colega Joseph Farrell me dijo que el director ejecutivo de Google deseaba reunirse conmigo, accedí a escucharle.

En cierto modo, los estratos superiores de Google me resultaban aún más distantes, impenetrables y oscuros que las salas de audiencia de Washington. Por aquel entonces ya hacía años que nos veníamos enfrentando a los altos funcionarios de Estados Unidos y su mística ya se había disipado, pero los centros de poder que crecían en Silicon Valley aún eran opacos, por lo que fui consciente de que se me presentaba una oportunidad de oro para intentar comprender e influir en la que se estaba convirtiendo en la compañía más influyente de la tierra. Schmidt había sido nombrado consejero delegado de Google en 2001, y había logrado convertirla en un imperio[1].

Me intrigaba sobremanera que la montaña estuviese dispuesta a acudir a Mahoma, pero hasta que Schmidt y su séquito no llegaron y se fueron no me di cuenta de quién me había visitado realmente.



La razón esgrimida como motivo de su visita fue un libro. Schmidt estaba redactando un tratado en colaboración con Jared Cohen, director de Google Ideas, un departamento de Google que se describía y se describe a sí mismo como un «comité interno de expertos teórico-prácticos». Por entonces yo sabía poco más que eso sobre Cohen. Lo cierto es que en 2010 se había

trasladado a Google desde el Departamento de Estado de Estados Unidos, donde, contratado con veinte y pocos años, había sido un creativo de la «Generación Y» con gran verborrea que trabajó bajo dos administraciones distintas, un cortesano del mundo de la creación de ideas políticas, que llegó a ocupar el cargo de asesor jefe de las secretarias de Estado Condoleezza Rice y Hillary Clinton. Como parte del Personal de Planificación Política, Cohen fue bautizado como «el organizador de fiestas de Condi», y se encargó de introducir los términos informáticos de moda en los círculos políticos de Estados Unidos, sacando de su chistera productos retóricos tan deliciosos como la «Diplomacia Pública 2.0»[2]. En la página adjunta de personal del Consejo de Relaciones Internacionales se incluyó como experto en «terrorismo; radicalismo; impacto de las tecnologías de comunicación en el arte de gobierno del siglo XXI; Irán»[3].

Fue el propio Cohen, según se dice, quien desde el Departamento de Estado contactó con el consejero delegado de Twitter, Jack Dorsey, para pedirle que demorase el mantenimiento programado con el fin de asistir al abortado alzamiento en Irán en 2009[4]. Su documentada relación amorosa con Google comenzó ese mismo año cuando conoció y se hizo amigo de Eric Schmidt durante la evaluación de los daños de la ocupación de Bagdad. Unos meses después, Schmidt recreó el hábitat natural de Cohen en el seno de Google creando el mencionado «comité interno de expertos teórico-prácticos», con base en Nueva York, y nombrando a Cohen como su director. Google Ideas acababa de nacer.

Ese mismo año, ambos escribieron conjuntamente un artículo para la revista bimensual del Consejo de Relaciones Internacionales, *Foreign Affairs*, en el que alababan el potencial reformador de las tecnologías de Silicon Valley como instrumento en la política exterior de Estados Unidos[5]. Describiendo lo que denominaban las «alianzas de los conectados»[6], Schmidt y Cohen afirmaban que:

> Los estados democráticos que han establecido alianzas entre sus sectores militares tienen la capacidad de hacer exactamente lo mismo con sus tecnologías de comunicación. […] Estas tecnologías ofrecen una nueva forma para ejercer el *deber de protección* a los ciudadanos de todo el mundo [cursiva añadida][7].

En dicho artículo también afirmaron que «con mucha diferencia, la mayor parte de esta tecnología procede del sector privado».

En febrero de 2011, menos de dos meses después de la publicación de este artículo, el presidente egipcio Hosni Mubarak fue depuesto por una revuelta popular. Hasta ese momento Egipto había sido un aliado de Estados Unidos, pues su dictadura militar contaba con el apoyo de Washington a cambio de que esta apoyase a su vez los «intereses geopolíticos estadounidenses en la región»[8]. Durante las primeras fases de la revolución, las élites políticas occidentales apoyaron a Mubarak. El vicepresidente Joe Biden, que apenas un mes antes había afirmado que Julian Assange era un «terrorista tecnológico», sostenía ahora que Hosni Mubarak no era un dictador, y recalcaba que no debería dimitir de su cargo[9]. El exprimer ministro británico Tony Blair insistía en que Mubarak era «inmensamente valiente y una fuerza del bien»[10]. En opinión de la secretaria de Estado Hillary Clinton, los Mubarak eran «amigos de la familia»[11].

Tal y como muestra una lectura atenta del flujo de sus comunicaciones internas, durante años el Departamento de Estado había estado apostando en secreto a ambos caballos, pues al tiempo que contribuía a mantener a Mubarak en el poder también apoyaba a ciertos elementos de la sociedad civil egipcia. Sin embargo, cuando Estados Unidos se percató de que la salida de Hosni era inevitable, se esforzó apresuradamente por encontrar alternativas. En primer lugar intentó impulsar a su sucesor preferido, Omar Suleiman, el odiado director de inteligencia interna, pero el corresponsal diplomático del Departamento de Estado en El Cairo, que por entonces colaboraba bastante con nosotros, publicó una sincera opinión sobre su historial político: Suleiman era el jefe de los torturadores de Egipto, el preferido de la CIA y también de Israel como sustituto de Mubarak[12]. Por estas y otras razones, Suleiman acabó perdiendo el apoyo internacional y los egipcios lo rechazaron igual que habían hecho con Mubarak. Como de costumbre poco deseoso de apoyar a un perdedor, Estados Unidos modificó su postura e intentó situarse al frente de la multitud; olvidó rápidamente su antigua vacilación, y el largo y difícil camino hacia la revolución egipcia fue considerado por Hillary Clinton como un triunfo para las corporaciones estadounidenses de tecnología, y posteriormente para el propio Departamento de Estado[13].

De repente todo el mundo deseaba estar en el punto de intersección entre el poder global de Estados Unidos y los medios de comunicación sociales, y Schmidt y Cohen ya se habían preocupado de vigilar de cerca el territorio. Con el título provisional de «El imperio de la mente», comenzaron a expandir su artículo hasta ir alcanzando poco a poco el tamaño de un libro y, como

parte de su investigación, trataron de contactar con personas importantes de la tecnología y el poder global.

Dijeron que deseaban entrevistarme, y yo accedí.

Se fijó fecha para el mes de junio.



Cuando llegó junio ya había mucho de lo que hablar. Ese verano WikiLeaks aún estaba ocupada con la revelación de comunicados diplomáticos estadounidenses, publicando miles de ellos cada semana. Siete meses antes, poco después de que comenzáramos a publicar estos comunicados, Hillary Clinton había denunciado esta publicación diciendo que era «un ataque a la comunidad internacional» que se proponía «dañar la estructura» del gobierno. En cierto modo, no le faltaba razón.

En muchos países, la «estructura» a la que se refería Clinton había sido construida con mentiras: cuanto más autoritario era el país, mayores eran las mentiras; cuanto más dependía de Estados Unidos una determinada fuerza política para afianzar su poder, más se quejaba esta ante sus apoyos estadounidenses acerca de sus rivales por el poder. Este patrón se repetía en capitales de todo el mundo: un caprichoso sistema global de lealtades secretas, favores debidos y falsos consensos, de decir una cosa en público y la contraria en privado. La escala y la diversidad geográfica de nuestras publicaciones superaron con creces la capacidad del Departamento de Estado para hacer frente a la crisis. Los vínculos entre los jugadores se quebraron, dejando grietas por las que podían colarse décadas de resentimiento[14].

Los «daños en la estructura» del gobierno aparecieron casi de inmediato en el norte de África, donde el 28 de noviembre de 2010, en medio de un entorno político ya considerablemente inestable, se publicaron los primeros comunicados. En Túnez, donde la corrupción del régimen de Zine el-Abidine Ben Ali no era ningún secreto, la población sufría pobreza generalizada, alto desempleo y represión gubernamental, mientras los favoritos del régimen organizaban ostentosas fiestas y cuidaban bien de sus amigos. Sin embargo, fue la propia documentación interna del Departamento de Estado sobre la decadencia del gobierno de Ben Ali la que desencadenó la ira pública y las llamadas a la rebelión entre la población tunecina. El ministro de propaganda de Ben Ali, Oussama Romdhani, confesaría más tarde que nuestras filtraciones fueron «el golpe de gracia, aquello que acabó definitivamente con el sistema de Ben Ali»[15]. El régimen comenzó a censurar las comunicaciones por Internet, enfureciendo aún más a la población:

WikiLeaks y las páginas web de los periódicos *Al Akhbar* y *Le Monde* desaparecieron del ciberespacio tunecino, reemplazados por el mensaje «Ammar 404: Página no encontrada». El blog online Nawaat.org se resistió y se dedicó a distribuir traducciones de los comunicados que estaban bajo el radar del sistema de censura tunecino. Durante veinte días la ira popular fue hirviendo a fuego lento hasta que, llevado hasta la desesperación por los corruptos funcionarios municipales, el 17 de diciembre el joven frutero Mohamed Bouazizi se quemó a lo bonzo en público; su muerte le convirtió en un mártir y un símbolo, y la rebelión abierta se extendió por las calles.

Las protestas continuaron hasta 2011. El 10 de enero, cuando Túnez aún estaba en plena revuelta, Hillary Clinton se embarcó en lo que ella misma describió como su «gira de disculpas» por WikiLeaks, empezando por Oriente Medio[16]. Cuatro días después cayó el gobierno tunecino; y once días después de este hecho la agitación civil se extendió a Egipto, y las imágenes de las protestas, sin posibilidad de bloqueo, fueron ofrecidas por la red vía satélite de la cadena Al Jazeera de Catar. En menos de un mes se produjeron «días de furia» y alzamientos civiles en Yemen, Libia, Siria y Baréin, y protestas a gran escala en Argelia, Irak, Jordania, Kuwait, Marruecos y Sudán; incluso en Arabia Saudí y en Omán hubo manifestaciones de descontento. 2011 se convirtió en un año de importantes despertares políticos, severas medidas y oportunistas intervenciones militares; en enero Muamar Gadafi denunció a WikiLeaks[17], pero no llegó a ver el final del año.

La oleada de furor revolucionario tardó poco en extenderse por Europa y otros lugares; para cuando me reuní con Schmidt en junio, la Puerta del Sol de Madrid estaba ocupada y los manifestantes se enfrentaban a la policía antidisturbios por toda España; había campamentos en Israel; Perú había tenido varias protestas y un cambio de gobierno[18]; el movimiento estudiantil en Chile había tomado las calles; el Capitolio estatal en Madison, Wisconsin, había sido sitiado por decenas de miles de personas defendiendo el derecho de los trabajadores[19]; y había motines en ciernes en Grecia y posteriormente en Londres.

Paralelamente a los cambios ocurridos en las calles, Internet estaba sufriendo una rápida transformación, pasando de ser un apático medio de comunicación a una especie de *demos*, un *pueblo* que compartía cultura, valores y aspiraciones, un lugar en el que tenía lugar la historia, con el que sus habitantes se identificaban y del que incluso sentían que *procedían*.

Todo el mundo había sido testigo del trato dispensado por el gobierno de Estados Unidos a la supuesta fuente de la filtración de los comunicados del

Departamento de Estado, Chelsea Manning. En junio, una campaña global, coordinada a través de Internet, había logrado presionar a dicho gobierno para que dejase de acosarla y torturarla[20].

El bloqueo financiero de Estados Unidos contra WikiLeaks había provocado masivas protestas por denegación de servicio, realizadas por la que hasta el momento había sido una apolítica juventud usuaria de Internet. Anonymous pasó de ser apenas un oscuro y poco conocido foco de protesta a convertirse en la punta de lanza de la emergente ideología política a través de Internet.

En un espectacular ejercicio de intrusión electrónica y publicación de información, algunos expertos en informática afines a la causa, operando bajo el estandarte de Anonymous, habían revelado la existencia de una campaña dirigida contra WikiLeaks y sus simpatizantes (incluyendo el reportero Glenn Greenwald), organizada y coordinada por un grupo de contratistas de seguridad privada en nombre del Bank of America, con un presupuesto de dos millones de dólares mensuales[21].

Por entonces, Barrett Brown, un joven periodista freelance de gran talento, había comenzado un trabajo de investigación sobre este eje de seguridad estatal que, en última instancia, le acabaría llevando a una cárcel federal[22]. La divisa virtual Bitcoin había pasado de no valer nada a alcanzar la paridad con el dólar[23]. Y ya en junio se podían leer en Internet términos como «Operación Rebelión Empire State» y «Día de Furia en Estados Unidos», los primeros signos del desencanto público que en septiembre se unirían para crear «Ocupa Wall Street».

El mundo entero estaba en llamas, pero los terrenos agrícolas de Ellingham Hall aún estaban en calma. Norfolk era un marco idílico, pero mi situación estaba muy lejos de ser igual de idílica, pues al estar retenido allí bajo arresto domiciliario me encontraba en desventaja táctica. WikiLeaks siempre había seguido el método de guerra de guerrillas en sus publicaciones: si atraíamos la vigilancia y la censura en una jurisdicción, nos trasladábamos a otra, atravesando fronteras como fantasmas. Sin embargo, en Ellingham me convertí en un activo inamovible en estado de sitio; ya no podíamos escoger nuestros terrenos de batalla, y se abrieron frentes desde todas partes, por lo que tuve que aprender a pensar como un general. Estábamos en guerra abierta.

Nuestra «base industrial» estaba siendo bombardeada. Secciones enteras de la infraestructura física y humana de WikiLeaks estaban despareciendo, a medida que los bancos nos imponían bloqueos financieros ilegales mientras

las compañías de comunicación, los gobiernos extranjeros y nuestras redes humanas debían soportar la presión de Washington. Aunque no se me acusaba de ningún crimen, el caso de mi extradición fue de apelación en apelación, consumiendo mis ahorros y mi tiempo, y amenazando con la posibilidad de que en cualquier momento WikiLeaks quedase decapitada[24].

Cada mes traía consigo la noticia de nuevos organismos gubernamentales involucrados. De hecho, llegó a haber tantas agencias estadounidenses y australianas implicadas que ambos países comenzaron a remitir sus comunicados internos a la «totalidad del gobierno»[25]; la «Sala de Guerra a WikiLeaks» del Pentágono, por ejemplo, se había apropiado por sí sola de más de cien personas[26]. En un momento dado se creó un gran jurado estadounidense contra nosotros, dirigido específicamente contra mí y contra mis colaboradores, y en la actualidad aún sigue en activo[27]. El FBI continuó rastreando nuestra extensa plantilla en busca de posibles informadores; repentinamente, mucha gente tenía impreso el logotipo de WikiLeaks en sus tarjetas de visita, pero en realidad no trabajaban *para* WikiLeaks.

Una larga lista de pelotas y aduladores también estaba llamando a mi puerta, intentando surfear la ola económica creada por el conflicto; cada uno de ellos deseaba aprovechar un momento de proximidad y convertirlo en un jugoso escándalo que poder vender a algún periódico sensacionalista o en un favor que pudiese reclamarse en el momento más beneficioso.

Todo cuanto podíamos hacer era mantener un perfil bajo y seguir luchando, por ejemplo, mediante el envío de 251 000 comunicados del Departamento de Estado de Estados Unidos, junto con miles de páginas de archivos secretos de la base de Guantánamo a más de cien países, todo un esfuerzo logístico, legal, cultural y político[28]. En los escasos momentos de pausa —debidos a una conexión a Internet poco fiable, que en ocasiones se cortaba a causa de la nieve— vigilábamos de cerca los cambios que se iban produciendo y reflexionábamos sobre el significado de todo ello. Prometíamos a nuestras fuentes un gran impacto, y no les estábamos defraudando; si alguno acababa en la cárcel, no habría sido en vano.



En el mes de junio, en este ambiente convulso, fue cuando Google se presentó ante mí, aterrizando en un aeropuerto de Londres y cubriendo en coche el largo trayecto hacia el este de Inglaterra hasta Norfolk y Beccles. Schmidt llegó el primero, acompañado por su entonces compañera, Lisa Shields, aunque cuando él me la presentó como vicepresidenta del Consejo de

Relaciones Internacionales —un comité de expertos estadounidenses especialistas en política exterior— tampoco le di excesiva importancia; Shields parecía recién salida de Camelot, y a principios de los años 90 se la pudo ver junto a John Kennedy Jr. Ambos se sentaron conmigo e intercambiamos cumplidos y bromas durante un tiempo de cortesía, pasado el cual me comunicaron que habían olvidado traer su dictáfono, por lo que tuvimos que utilizar el mío, acordando que yo les enviaría la grabación y ellos a su vez me remitirían la transcripción para su revisión a efectos de exactitud y claridad. Nada más comenzar, Schmidt se lanzó sin miramientos a la parte más honda de la piscina, interrogándome sin tapujos acerca de las bases organizativas y tecnológicas de WikiLeaks.

Poco tiempo después llegaron Jared Cohen y un tal Scott Malcomson, el editor del libro. Tres meses después de la reunión, Malcomson sería nombrado jefe de redactores de discursos en el Departamento de Estado y principal asesor de Susan Rice (entonces embajadora de Estados Unidos ante las Naciones Unidas y actualmente consejera de Seguridad Nacional); anteriormente había sido asesor senior en la ONU, y durante muchos años ha sido miembro permanente del Consejo de Relaciones Internacionales. En el momento de escribir este libro, trabaja como director de comunicaciones en el Grupo de Crisis Internacionales[29].

En aquel momento, la delegación era una cuarta parte Google y tres cuartas partes del departamento de política exterior de Estados Unidos, pero yo eso aún lo ignoraba. Cumplidos los apretones de manos de rigor, nos metimos rápidamente en materia.

Schmidt demostró ser un formidable entrevistador. A sus cincuenta y muchos años, ligeramente bizco tras sus grandes anteojos y vestido a la antigua, su adusta y taciturna apariencia ocultaba la mente analítica de una máquina. Sus preguntas se dirigían a menudo al corazón mismo del asunto, revelando una poderosa inteligencia estructural, el mismo intelecto que había logrado abstraer los principios de ingeniería de *software* para convertir a Google en una megaempresa, asegurándose de que la infraestructura corporativa siempre estuviese a la altura de la tasa de crecimiento. Era una persona que sabía perfectamente cómo construir y mantener *sistemas*: sistemas de información y sistemas de personas. Mi mundo era nuevo para él, pero también era un mundo de procesos humanos en desarrollo, escalas y flujos de información.

Para ser un hombre de inteligencia tan sistemática, las ideas políticas de Schmidt —por lo que pude inferir de nuestra discusión— eran

sorprendentemente convencionales, incluso banales. Entendía con rapidez las relaciones estructurales, pero le costaba mucho verbalizar buena parte de ellas, a menudo tenía que meter con calzador las sutilezas geopolíticas en la jerga mercantil de Silicon Valley o en el osificado microlenguaje de sus compañeros, típico del Departamento de Estado[30]. Cuando realmente se encontraba en su elemento era cuando hablaba (tal vez sin ser consciente de ello) como un ingeniero, fragmentando las complejidades en sus componentes ortogonales.

Cohen me pareció un buen oyente, pero un pensador menos interesante, poseedor de esa incansable cordialidad que se ve con frecuencia en generalistas de carrera y académicos de Rhodes. Como era de esperar dado su historial en política exterior, Cohen tenía un buen conocimiento de los puntos candentes y los conflictos internacionales, y se movía con soltura de uno a otro, detallando diferentes situaciones hipotéticas para poner a prueba mis afirmaciones. Sin embargo, en ocasiones daba la impresión de que se extendía en exposiciones ortodoxas de una forma que parecía diseñada para impresionar a sus antiguos colegas en el ámbito oficial de Washington. Malcomson, más mayor, era más reflexivo, y sus aportaciones eran meditadas y generosas. Shields permaneció en silencio durante la mayor parte de la conversación, tomando notas y siguiéndoles el juego a los mayores egos presentes alrededor de la mesa, mientras hacía el verdadero trabajo.

En tanto que entrevistado, lógicamente se esperaba de mí que llevase el peso de la conversación, y a lo largo de las horas que pasamos juntos intenté guiar a mis interlocutores hacia mi visión del mundo. Para gran mérito suyo, considero que aquella fue tal vez la mejor entrevista que me han hecho nunca. Me encontré todo el tiempo fuera de mi zona de confort, y eso me gustó. Tras un ligero almuerzo dimos un paseo por los campos adyacentes, siempre con la grabadora en marcha. Pedí a Schmidt que filtrase a WikiLeaks peticiones de información realizadas a Google por el gobierno de Estados Unidos, y él se negó, súbitamente nervioso, aludiendo a la ilegalidad de revelar peticiones según la Patriot Act. Finalmente, llegó la noche y todo terminó; se marcharon de vuelta a las irreales y remotas salas de audiencias del imperio de la información, y yo me quedé para ocuparme nuevamente de mi trabajo. Fue el final de todo aquel asunto, o eso pensé.



Dos meses después, la publicación de los comunicados del Departamento de Estado por parte de WikiLeaks llegó abruptamente a su fin. Durante nueve

meses habíamos gestionado cuidadosamente la progresiva publicación, atrayendo a más de cien medios de comunicación de todo el mundo, distribuyendo los documentos en sus regiones de influencia, y supervisando un sistema global y sistemático de publicación y redacción, con vistas a lograr el máximo impacto para cada fuente.

Sin embargo, en un acto de suprema negligencia, el periódico *The Guardian* —antiguo colaborador nuestro— había revelado la contraseña confidencial para el descifrado de los 251 000 comunicados en el título de un capítulo de su libro, publicado apresuradamente en febrero de 2011[31]. A mediados de agosto descubrimos que un antiguo empleado alemán —al que yo mismo había despedido en 2010— estaba manteniendo relaciones comerciales con un amplio abanico de organizaciones e individuos para intentar vender al mejor postor la localización del archivo codificado y de la contraseña que aparecía en el libro. Al ritmo al que se estaba difundiendo esta información, estimamos que en menos de dos semanas todas las agencias de inteligencia, contratistas e intermediarios tendrían acceso a todos los comunicados, pero el gran público no.

Entonces llegué a la conclusión de que era necesario dar a conocer nuestro programa de publicaciones para los próximos cuatro meses y contactar con el Departamento de Estado para que quedase constancia de que les habíamos advertido con suficiente antelación, y de esta forma impedir que se produjese otro ataque legal o político. Incapaces de contactar con Louis Susman, por entonces embajador estadounidense en el Reino Unido, probamos entonces a llamar a la puerta principal. La directora de investigaciones de WikiLeaks, Sarah Harrison, contactó entonces con el Departamento del Tesoro e informó al operador que «Julian Assange» deseaba hablar con Hillary Clinton. Como era de prever, esta información fue recibida inicialmente con incredulidad burocrática, y pronto nos encontramos representando una nueva versión de la famosa escena de *¿Teléfono rojo? Volamos hacia Moscú*, en la que uno de los personajes interpretados por Peter Sellers llama por teléfono a la Casa Blanca para informar de una inminente guerra nuclear e inmediatamente es puesto en espera. Al igual que en la película, fuimos poco a poco escalando la jerarquía, hablando con funcionarios de rango creciente hasta llegar al jefe de asesores legales de Clinton, quien nos dijo que nos llamaría en breve. Colgamos el teléfono y esperamos pacientemente.

Cuando sonó el teléfono media hora más tarde, la persona que estaba al otro lado de la línea no pertenecía al Departamento de Estado, sino que se trataba de Joseph Farrell, el empleado de WikiLeaks que había organizado la

entrevista con Google, y que al parecer acababa de recibir un correo electrónico de Lisa Shields pidiéndole confirmación de que realmente era WikiLeaks quien trataba de contactar con el Departamento de Estado.

En ese preciso momento me di cuenta de que era muy posible que Eric Schmidt no hubiera sido únicamente un emisario de Google. De manera oficial o no, Schmidt mantenía contactos que le situaban muy cerca de Washington D. C., incluyendo una relación bien documentada con el presidente Obama en persona. No solo la gente de Hillary Clinton sabía que la compañera de Schmidt me había visitado, sino que la habían escogido como canal de comunicación oculto. Mientras WikiLeaks había estado muy ocupada publicando los archivos internos del Departamento de Estado estadounidense, este había logrado a su vez introducirse sigilosamente en el centro del mando de WikiLeaks para invitarme a comer. Dos años después, durante las visitas que realizó a China, Corea del Norte y Myanmar a comienzos de 2013, quedaría bastante claro que el presidente de Google estaba llevando a cabo, de un modo u otro, «diplomacia encubierta» para Washington. Sin embargo, en aquel momento era algo totalmente novedoso[32].

Lo cierto es que me olvidé de todo esto hasta febrero de 2012, cuando WikiLeaks —junto con más de treinta de nuestros colaboradores mediáticos internacionales— comenzó a publicar los Archivos de Inteligencia Global: los correos electrónicos internos de la agencia privada de inteligencia Stratfor[33], radicada en Texas. Uno de nuestros colaboradores de investigación más sólidos —el periódico *Al Akhbar*, con base en Beirut— revisó minuciosamente estos correos electrónicos en busca de información relacionada con Jared Cohen[34]. La gente de Stratfor, a la que le gustaba considerarse como una especie de CIA corporativa, era extremadamente consciente de que otras compañías estaban comenzando a entrar en su sector, siendo Google la que más llamó la atención en su radar. En una serie de llamativos correos discutían el carácter de las actividades llevadas a cabo por Cohen bajo la égida de Google Ideas, preguntándose a qué se refiere exactamente la parte «práctica» del «comité de expertos teórico-prácticos».

La actividad directiva de Cohen parecía pasar de las relaciones públicas y el trabajo de «responsabilidad corporativa» a la intervención corporativa directa y activa en asuntos exteriores a un nivel normalmente reservado a los países, por lo que Jared Cohen podía muy bien ser considerado irónicamente como «director de cambio de régimen». De acuerdo con los correos electrónicos, estaba intentando dejar su huella en alguno de los grandes

acontecimientos históricos del Oriente Medio contemporáneo. Por ejemplo, se le pudo localizar en Egipto en algún momento de la revolución, donde se reunió con Wael Ghonim, el empleado de Google cuyo arresto y encarcelamiento horas después le convertiría en un símbolo del alzamiento para la prensa occidental. Además, se habían planeado otras reuniones en Palestina y Turquía, aunque ambas —siempre según los correos de Stratfor— fueron anuladas por la junta directiva de Google al considerarlas demasiado arriesgadas. Unos pocos meses antes de conocerme, Cohen estaba planeando un viaje a la frontera entre Azerbaiyán e Irán para «entablar relaciones con las comunidades iraníes más próximas a la frontera», actividad que formaba parte de un proyecto de Google Ideas sobre las «sociedades represivas». En un correo interno, el vicepresidente del Departamento de Inteligencia de Stratfor, Fred Burton (antiguo especialista en seguridad del Departamento de Estado), escribió:

Google cuenta con el apoyo y la cobertura aérea de la CB [Casa Blanca] y del Departamento de Estado. La realidad es que están haciendo cosas que ni siquiera la CIA está en condiciones de hacer […]. [Cohen] va a acabar logrando que le secuestren o le maten, y es posible que esto sea lo mejor que pudiera ocurrir para revelar al mundo el papel que Google está realizando en secreto para «inflar» los alzamientos, por decirlo sin tapujos. De este modo, si algo sale mal, el gobierno de EE. UU. puede negar todo conocimiento del tema y es Google quien se queda con el marrón[35].

En otros comunicados internos, Burton aseguraba que sus fuentes sobre las actividades de Cohen eran Marty Lev —director de seguridad de Google— y el propio Eric Schmidt[36].

Intentando encontrar algo un poco más concreto, comencé a buscar en el archivo de WikiLeaks información sobre Jared Cohen. Algunos de los comunicados del Departamento de Estado publicados como parte del conocido «Cablegate» revelan que Cohen había estado en Afganistán en 2009, tratando de convencer a las cuatro compañías de telefonía móvil afganas de que trasladasen sus antenas y equipos de transmisión a las bases militares estadounidenses[37]. En Líbano trabajó en secreto para crear e instaurar un rival intelectual y clerical de Hezbolá, la «Liga Chiita»[38]. Y en Londres ofreció a los ejecutivos cinematográficos de Bollywood fondos para

introducir contenidos antiextremistas en sus películas, prometiendo ponerles en contacto con redes relacionadas en Hollywood[39].

Tres días después de visitarme en Ellingham Hall, Jared Cohen tomó un vuelo a Irlanda para dirigir la «Cumbre contra el Extremismo Violento», un encuentro internacional patrocinado por Google Ideas y el Consejo de Relaciones Internacionales. Reuniendo a antiguos miembros de bandas callejeras, militantes de extrema derecha, violentos nacionalistas y «extremistas religiosos» de todo el mundo en un mismo lugar, el evento aspiraba a idear y desarrollar soluciones tecnológicas para el problema del «extremismo violento»[40]. ¿Qué podía salir mal?

El mundo de Cohen parece estar formado exclusivamente por eventos como este, uno detrás de otro: interminables veladas en busca del intercambio cruzado de influencias entre las élites y sus vasallos, todos ellos reunidos bajo el piadoso epígrafe de «sociedad civil». En el imaginario popular de las sociedades capitalistas avanzadas se mantiene la creencia de que aún existe un «sector de la sociedad civil» que se organiza de manera autónoma y que se reúne para manifestar los intereses y la voluntad de los ciudadanos. Según esta fábula, el ámbito de actuación de este sector cuenta con el respeto del gobierno y el «sector privado», dejando un cómodo espacio de seguridad en el que las ONG y las entidades sin ánimo de lucro pueden defender cosas tan importantes como los derechos humanos, la libertad de expresión y las responsabilidades del gobierno.

Sobre el papel, este esquema parece una gran idea, pero si alguna vez fue posible desde luego no ha sido el caso desde hace varias décadas. Al menos desde los años 70, actores tan legítimos como los sindicatos y las iglesias han tenido que plegarse ante los continuos ataques del estatismo del libre mercado, transformando la «sociedad civil» en un mercado en el que las distintas facciones políticas y los intereses corporativos ejercen su influencia desde una cómoda distancia. Los últimos cuarenta años han sido testigos de una enorme proliferación de «comités de expertos» y ONG políticas cuyo propósito, bajo una atractiva verborrea, no es otro que ejecutar agendas políticas por poderes.

No se trata únicamente de los conocidos grupos *neocon* como Iniciativa de Política Exterior[41], sino que también hay que incluir fatuas ONG occidentales como Freedom House («Casa de la Libertad»), cuyos ingenuos pero bienintencionados trabajadores voluntarios viven hechos un lío por las políticas que les imponen sus fuentes de financiación, denunciando violaciones de los derechos humanos en países no occidentales y haciendo

caso omiso de los abusos locales. El circuito de conferencias sobre temas relacionados con la sociedad civil —que obliga a los activistas de los países en desarrollo a viajar por todo el mundo cientos de veces al año para bendecir la profana unión entre «gobiernos y accionistas privados», en eventos geopolitizados como el «Foro de Internet de Estocolmo»— sencillamente no podría existir si no contase con los millones de dólares de financiación política que recibe anualmente.

Si se leen con atención las listas de miembros de los grupos de expertos e institutos más grandes e importantes de Estados Unidos se puede comprobar que los mismos nombres aparecen de forma bastante recurrente. La cumbre contra el extremismo violento organizada por Cohen fue el germen de AVE, o AgainstViolent-Extremism.org, un proyecto a largo plazo cuyo principal patrocinador, aparte de Google Ideas, es Gen Next Foundation. La página web de esta fundación afirma de sí misma que es «una organización de miembros exclusivos y una plataforma de lanzamiento para individuos de éxito» que aspira a lograr el «cambio social» utilizando fondos de capital riesgo[42]; «El sector privado y la financiación sin ánimo de lucro» de Gen Next «logra evitar algunos de los conflictos potenciales de intereses generados por iniciativas financiadas por los gobiernos»[43]. Jared Cohen es miembro ejecutivo de esta fundación.

Gen Next también presta apoyo a una ONG creada por Cohen en su última etapa en el Departamento de Estado, cuyo principal objetivo es introducir las campañas mundiales por Internet de los «activistas prodemocracia» en la red de mecenazgo de Estados Unidos para relaciones internacionales[44]. Este organismo inició sus actividades en 2008 con el nombre de «Alliance of Youth Movements» (Alianza de los Movimientos de la Juventud) y realizó una cumbre inaugural en Nueva York, financiada por el Departamento de Estado y numerosos patrocinadores privados[45]. La cumbre contó con la presencia de activistas sociales cuidadosamente escogidos, procedentes de «áreas problemáticas» como Venezuela y Cuba, que asistieron a los discursos del equipo de nuevos medios de comunicación de Obama y de James Glassman, del Departamento de Estado, y se esforzaron por crear redes de colaboración con consultores de relaciones públicas, «filántropos» y personalidades de los medios estadounidenses[46].

El grupo organizó otras dos cumbres solo para invitados escogidos en Londres y México D. F., en las que Hillary Clinton se dirigió a los delegados por videoconferencia[47]:

Ustedes constituyen la vanguardia de una generación en ascenso de ciudadanos activistas. […] Y eso los convierte en la clase de líderes que necesitamos[48].

En 2011, la Alliance of Youth Movements cambió su nombre por el de «Movements.org», y en 2012 se convirtió en una división de «Advancing Human Rights» (Progreso de los Derechos Humanos), una nueva ONG creada por Robert L. Bernstein tras abandonar Human Rights Watch, organización que él mismo había fundado, porque en su opinión no debería ocuparse de los abusos de derechos en Israel y Estados Unidos[49]. El objetivo principal de Advancing Human Rights consiste en corregir la desviación de Human Rights Watch, centrándose exclusivamente en «dictaduras»[50].

Cohen declaró que la fusión de su grupo Movements.org con Advancing Human Rights era «irresistible» debido a «la fantástica red de ciberactivistas en Oriente Medio y el norte de África de AHR»[51]. Poco después se unió al consejo de administración de este último organismo, donde también se encuentra Richard Kemp, excomandante de las fuerzas británicas en Afganistán[52]. Actualmente, Movements.org continúa recibiendo financiación de Gen Next, así como de Google, de MSNBC y del gigante de relaciones públicas Edelman, que representa a General Electric, Boeing y Shell, entre otras compañías[53].

Google Ideas es más grande, pero sigue exactamente el mismo plan, como lo demuestra una simple ojeada a la lista de ponentes de sus exclusivos encuentros anuales, como por ejemplo «Crisis en un mundo conectado», celebrado en octubre de 2013. Los teóricos y activistas de las redes sociales recubren el evento con una pátina de autenticidad, pero en realidad los asistentes conforman una piñata bastante tóxica: funcionarios gubernamentales, magnates de las telecomunicaciones, consultores en materia de seguridad, capitalistas financieros y buitres tecnológicos especialistas en política exterior como Alec Ross (gemelo de Cohen en el Departamento de Estado)[54]. En el núcleo duro central se encuentran los contratistas de armas y los militares de carrera: jefes de mando en el ciberespacio de Estados Unidos, e incluso el almirante responsable de todas las operaciones militares estadounidenses en América Latina desde 2006 hasta 2009. Como guinda del pastel, se encuentran Jared Cohen y el presidente de Google, Eric Schmidt[55].

En un momento dado comencé a pensar que Schmidt era un multimillonario del sector tecnológico californiano, brillante pero poco ducho en lo político, que estaba siendo utilizado por los mismos especialistas en

política exterior estadounidense que había reclutado para que hiciesen las veces de intérpretes entre él y el Washington oficial, una especie de ilustración Costa Oeste-Costa Este del dilema principal-agente[56].

Me equivocaba.



Eric Schmidt nació en Washington D. C., donde su padre trabajó como profesor y economista en el Departamento del Tesoro de Richard Nixon. Fue al instituto en Arlington, y después se graduó en ingeniería en Princeton en 1979, desde donde saltó a la Costa Oeste para obtener un doctorado en Berkeley y entrar a trabajar en 1983 en Sun Microsystems, filial de Stanford/Berkeley. Tan solo dieciséis años después, Schmidt abandonó la empresa tras haber entrado a formar parte de la dirección ejecutiva.

Sun Microsystems tenía firmados importantes contratos con el gobierno de Estados Unidos, pero los archivos muestran que Schmidt no se relacionó estratégicamente con la clase política de Washington hasta que llegó a Utah para asumir el cargo de consejero delegado de Novell. El archivo financiero de las campañas electorales federales revela que el 6 de enero de 1999 Schmidt donó dos lotes de 1000 dólares al senador republicano por Utah Orrin Hatch, y ese mismo día su esposa Wendy también hizo una donación de dos lotes de 1000 dólares al senador Hatch. A comienzos de 2001, más de una docena de políticos y CAP (entre ellos, Al Gore, George W. Bush, Dianne Feinstein y Hillary Clinton) habían sido financiados por Schmidt, alcanzando en uno de los casos la suma de 100 000 dólares[57]. Para el año 2013, Eric Schmidt —que se había asociado de forma notoriamente pública con la Casa Blanca de Obama— estaba metido hasta el fondo en la financiación política: ocho republicanos, ocho demócratas y dos CAP habían recibido directamente sus fondos; ese mes de abril, 32 300 dólares entraron en la cuenta del Comité Nacional Republicano del Senado, y apenas un mes después otros 32 300 dólares entraron en la cuenta del Comité de Campaña Demócrata del Senado. La razón de donar exactamente esa misma cantidad a ambos partidos era que, en aquel momento, tal cantidad era la máxima que un individuo podía donar a un comité de partido, y deseaba asegurarse el agradecimiento de los dos más importantes[58].

En 1999, Schmidt también se unió al consejo de administración de un grupo radicado en Washington D. C.: la New America Foundation, una fusión de diversas fuerzas centristas bien conectadas entre sí (al menos en términos de la capital de Estados Unidos). La fundación y sus 100 empleados

funcionan como un grupo de presión, que utiliza sus redes homologadas en materia de seguridad nacional, de política exterior y de especialistas en tecnología para publicar cientos de artículos y columnas de opinión cada año. En 2008, Schmidt fue nombrado presidente de dicho consejo de administración, y en 2013 los principales proveedores de fondos de la fundación son Eric y Wendy Schmidt (con más de un millón de dólares cada uno), el Departamento de Estado de Estados Unidos y la Fundación Bill y Melinda Gates; entre los proveedores secundarios se cuentan Google, la Agencia de Estados Unidos para el Desarrollo Internacional (la USAID, por sus siglas en inglés) y Radio Free Asia[59].

El grado de implicación de Schmidt en la New America Foundation le sitúa claramente como muy próximo a la élite política de Washington. Entre el resto de miembros del consejo de administración de la fundación, siete de los cuales también forman parte del Consejo de Relaciones Internacionales, se incluyen las siguientes personas: Francis Fukuyama, uno de los padres intelectuales del movimiento neoconservador; Rita Hauser, que trabajó en el consejo asesor de inteligencia de los presidentes Bush y Obama; Jonathan Soros, hijo de George Soros; Walter Russell Mead, un estratega de la seguridad estadounidense y editor de la revista *The American Interest*; Helene Gayle, miembro también de los consejos de administración de Coca-Cola, Colgate-Palmolive, la Rockefeller Foundation, la Unidad de Política Exterior del Departamento de Estado, el Consejo de Relaciones Internacionales, el Centro de Estudios Estratégicos e Internacionales, el programa Fellow de la Casa Blanca y de la Campaña ONE del cantante Bono; y Daniel Yergin, geoestratega del petróleo, antiguo director de la Comisión sobre Estrategia de la Investigación Energética del Departamento de Energía de Estados Unidos y autor del libro *Historia del Petróleo*[60].

La directora ejecutiva de la fundación, nombrada en 2013, es la antigua jefa de Jared Cohen en la sección de planificación de políticas en el Departamento de Estado, Anne-Marie Slaughter, especialista en derecho y relaciones internacionales, licenciada en Princeton y con muy buen ojo para detectar puertas giratorias[61]. En el momento de escribir este libro se ha hecho casi omnipresente, haciendo llamamientos a Obama para que responda a la crisis de Ucrania no solo desplegando en secreto fuerzas estadounidenses en el país, sino también bombardeando Siria, pues ello enviaría un mensaje muy claro a Rusia y a China[62]. Al igual que Schmidt, asistió a la Conferencia Bilderberg de 2013 y forma parte del Consejo de Administración de Política Exterior del Departamento de Estado[63].

Eric Schmidt era cualquier cosa menos un lego en temas políticos. Mi error fue estar demasiado deseoso de ver en él a un ingeniero de Silicon Valley sin ambición política, una reliquia de la cultura tradicional de especialistas en ciencia informática de la Costa Oeste. Sin embargo, ese tipo de persona no suele asistir a las conferencias Bilderberg durante cuatro años seguidos, ni visitar regularmente la Casa Blanca, ni ofrecer «charlas junto al fuego» en el Foro Económico Mundial en Davos[64]. El ascenso de Schmidt a «ministro de asuntos exteriores» de Google —llevando a cabo ceremoniosas visitas de estado a puntos geopolíticos candentes— no surgió de la nada, sino que había sido precedido por años de integración en las redes más reputadas e influyentes de Estados Unidos.

A nivel humano, Schmidt y Cohen son dos personas totalmente encantadoras, pero el presidente de Google es el clásico «jefe de empresa», con todo el bagaje cultural que viene asociado a este papel[65]. Schmidt encaja perfectamente en el lugar en el que se encuentra: el punto en el que las tendencias centristas, liberales e imperialistas se encuentran con la vida política estadounidense. Da toda la impresión de que los jefes de Google creen genuinamente en el poder civilizador de las iluminadas corporaciones multinacionales, y consideran esta misión como parte de la remodelación del mundo de acuerdo con el mejor criterio de la «benevolente superpotencia». Sin duda dirán a todo el que pregunte que la apertura de mente y la ausencia de prejuicios es una virtud, pero que toda perspectiva que amenace la prepotencia que guía la política exterior de Estados Unidos es y será siempre invisible para ellos. Esto es la increíble banalidad del «No seas malo»: están convencidos de que están haciendo el bien. Y eso es un problema: Google es diferente, Google es visionario, Google es el futuro, Google es más que una simple compañía, Google vela por la comunidad, Google es una fuerza del bien.



Incluso cuando Google airea públicamente su ambivalencia corporativa, estos preceptos de fe nunca se ven alterados[66], pues la reputación de la compañía es prácticamente inexpugnable. Su logotipo, colorista y juguetón, está impreso en las retinas de casi seis mil millones de visitantes diarios, es decir, 2,1 billones anuales, lo que supone una capacidad de condicionamiento del usuario que no tiene ni ha tenido jamás ninguna empresa actual o del pasado[67]. A pesar de haber sido descubierta ofreciendo petabytes de datos personales a la comunidad de servicios de inteligencia estadounidense a

través del programa PRISM, Google salvó la cara sin esfuerzo gracias a la benevolencia generada por su ambiguo discurso del «No seas malo»: algunas cartas abiertas, meramente simbólicas, dirigidas a la Casa Blanca y todo pareció quedar olvidado. Ni siquiera los detractores de la vigilancia encubierta han podido resistirse al hechizo de Google, pues condenan inmediatamente al gobierno por supuesto espionaje pero minimizan las invasivas prácticas de Google mediante técnicas de contemporización[68].

Nadie desea reconocer que Google se ha vuelto grande y malo, pero así es. El periodo de Schmidt como presidente y consejero delegado ha visto cómo Google, a medida que ha ido convirtiéndose en una megacorporación geográficamente invasiva, se ha ido integrando en las estructuras de poder más turbias de Estados Unidos. Sin embargo, Google siempre se ha sentido confortable con esa proximidad al poder; de hecho, mucho antes de que los fundadores de la compañía, Larry Page y Sergey Brin, contratasen a Schmidt en 2001, la investigación inicial en la que se basaron para crear Google fue financiada por la Agencia de Proyectos de Investigación Avanzada sobre Defensa (en inglés, la DARPA)[69]. Y al mismo tiempo que el Google de Schmidt desarrollaba su imagen de gigante de la tecnología global extremadamente amigable, también construía una sólida relación con los organismos de inteligencia.

En 2003, la Agencia de Seguridad Nacional (ASN) de Estados Unidos, bajo la dirección de Michael Hayden, ya había comenzado a violar sistemáticamente la Ley de Vigilancia de Inteligencia Exterior (en inglés, la FISA)[70], con el programa denominado «Conocimiento Total de Información»[71]. Incluso antes de que se ideara el famoso programa PRISM por orden de la administración Bush, la ASN ya aspiraba a «recopilarlo todo, olfatearlo todo, saberlo todo, procesarlo todo y explotarlo todo»[72]. Durante ese mismo periodo, Google —cuya misión corporativa declarada era la de recopilar y «organizar la información mundial, convirtiéndola en algo universalmente accesible y útil»[73]— aceptaba hasta 2 millones de dólares procedentes de la ASN para que proporcionase a la agencia las herramientas de búsqueda necesarias para acumular rápidamente información robada[74].

En 2004, tras absorber Keyhole, una empresa de «mapeado» tecnológico fundada por la Agencia Nacional de Inteligencia Geoespacial (en inglés, la NGA) y por la CIA, Google desarrolló la tecnología convirtiéndola en el hoy archiconocido Google Maps, y vendió una versión empresarial de tal tecnología al Pentágono y a agencias federales y estatales asociadas por medio de contratos multimillonarios[75]. En 2008, Google ayudó a lanzar al

espacio un satélite espía de la NGA, el GeoEye-1, y desde entonces comparte las fotografías realizadas por dicho satélite con el ejército de Estados Unidos y los organismos de inteligencia[76]. En 2010, la NGA concedió a Google un contrato de 27 millones de dólares a cambio de «servicios de visualización geoespacial»[77].

En 2010, después de que el gobierno chino fuese acusado de *hackear* la página web de Google, la compañía inició una relación de «intercambio formal de información» con la ASN, que supuestamente permitiría a los analistas de esta última «evaluar vulnerabilidades» en el *hardware* y el *software* de Google[78]. Aunque los detalles exactos del acuerdo nunca han sido revelados, la ASN incluyó en el mismo a otros organismos gubernamentales en concepto de asistencia técnica, entre ellos el FBI y el Departamento de Seguridad Nacional.

Más o menos al mismo tiempo, Google se estaba involucrando cada vez más en un programa conocido como «Marco de Seguridad Duradero»[79] (en inglés, el ESF), cuyo objetivo es compartir información entre las compañías tecnológicas de Silicon Valley y las agencias asociadas al Pentágono «a la velocidad de Internet»[80]. Los correos electrónicos relativos al ESF, obtenidos por peticiones amparadas en el derecho a la libertad de información, muestran que Schmidt y su colega en Google Sergey Brin mantenían una correspondencia de tuteo, llamándose por sus nombres de pila, con el director de la ASN, el general Keith Alexander[81]. Los informes sobre estos correos electrónicos hacían hincapié en la familiaridad del trato en la correspondencia: «¡General Keith! […] ¡Cómo me alegro de verte! […]», escribió Schmidt. Sin embargo, la mayoría de dichos informes pasaron por alto un detalle crucial: «Los conocimientos que te proporciona el ser miembro clave de la Base Industrial de Defensa», escribió Alexander a Brin, «son realmente valiosos a la hora de garantizar que los esfuerzos del ESF tengan un impacto apreciable».

El Departamento de Seguridad Nacional define la Base Industrial de Defensa como «el complejo industrial a nivel mundial que posibilita la investigación y el desarrollo, así como el diseño, la producción, el envío y el mantenimiento de sistemas, subsistemas y componentes o partes de armamento militar, *conforme a los estándares exigidos por el ejército de Estados Unidos* [énfasis añadido]»[82]. Esta Base Industrial de Defensa proporciona «productos y servicios esenciales para movilizar, desplegar y sostener operaciones militares». ¿Incluye esto los servicios comerciales comprados habitualmente por el ejército estadounidense? No; la definición

excluye específicamente la compra de estos servicios. Sea lo que sea lo que hace de Google un «miembro clave de la Base Industrial de Defensa» no son las campañas de reclutamiento realizadas a través de Google AdWords ni el uso de Gmail por los soldados.

En 2012, Google obtuvo un puesto en la lista de los grupos de presión con mayor nivel de gasto en Washington D. C., una lista habitualmente copada únicamente por la Cámara de Comercio de Estados Unidos, contratistas militares y los leviatanes del petróleo y el carbón[83]. Google entró en esta exclusiva lista en un puesto situado por encima del gigante de productos militares aeroespaciales Lockheed Martin, con un gasto total de 18,2 millones de dólares, frente a los 15,3 millones de Lockheed; Boeing, el contratista militar que absorbió McDonnell Douglas en 1997, también se situó por debajo de Google en gasto (15,6 millones de dólares), al igual que Northrop Grumman (17,5 millones).

En otoño de 2013, la administración Obama intentó conseguir apoyo para los ataques aéreos estadounidenses a Siria. A pesar de los reveses y contratiempos obtenidos, dicha administración continuó presionando en pos de las intervenciones militares hasta bien entrado septiembre, con discursos y declaraciones públicas del presidente Obama y del secretario de Estado John Kerry[84]. El 10 de septiembre, Google cedió su página principal —la más popular de todo Internet— para publicitar los esfuerzos bélicos, insertando una línea bajo la caja de búsqueda: «¡En directo! El secretario Kerry responde a preguntas sobre Siria. Hoy a través de Hangout a las 2 p. m., hora de la Costa Este»[85].

Tal y como escribió en 1999 Tom Friedman, el autodenominado «centrista radical»[86] y columnista de *The New York Times*, en ocasiones no basta con dejar la supremacía mundial de las corporaciones tecnológicas estadounidense a algo tan volátil como «el libre mercado»:

> La mano invisible del mercado no funcionará nunca sin la existencia de un puño invisible: McDonald's no puede florecer sin McDonnell Douglas, diseñador de los cazas F-15; y el puño invisible que mantiene una seguridad global para que florezcan las tecnologías de Silicon Valley está formado por el ejército, la fuerza aérea, la armada y el cuerpo de marines de Estados Unidos[87].

Si algo ha cambiado desde que se escribieron estas palabras es que Silicon Valley está cada vez más incómodo con el rol pasivo que se le ha asignado, y

aspira, en su lugar, a adornar el puño invisible con un guante de terciopelo. En 2013, Schmidt y Cohen escribieron que:

La tecnología y la ciberseguridad son al siglo XXI lo que Lockheed Martin fue al siglo XX[88].

Una forma de verlo es simplemente considerarlo como un negocio. Si un monopolio estadounidense de servicios por Internet desea garantizar su dominio global del mercado no puede limitarse a hacer su trabajo y dejar de lado la política. La hegemonía estratégica y económica de Estados Unidos es un pilar imprescindible de su primacía comercial. ¿Qué debe hacer una megacorporación? Si desea cabalgar a lomos del mundo, debe pasar a formar parte del genuino imperio del «No seas malo».

No obstante lo dicho, parte de la casi irrompible imagen de Google como «más que una simple compañía» procede de la percepción de que no actúa como una corporación grande y malvada. Por su tendencia a atraer a la gente hacia la trampa de sus servicios ofreciendo gigabytes de «almacenamiento gratuito», da la impresión de que Google entrega servicios sin coste, actuando en contradicción directa con el principal objetivo de toda empresa: el beneficio. Google está considerada como una compañía esencialmente filantrópica, una entidad mágica presidida por visionarios de fuera de este mundo y dispuesta a crear un futuro utópico[89]. En ocasiones, la compañía ha dado la impresión de estar ansiosa por cultivar esta imagen, financiando abundantemente iniciativas de «responsabilidad corporativa» con el fin de lograr «cambios sociales» (Google Ideas es el mejor ejemplo de ello). Pero tal y como muestra precisamente Google Ideas, los esfuerzos «filantrópicos» de la empresa se acercan peligrosamente a la parte imperial de la influencia de Estados Unidos. Si Blackwater/Xe Services/Academi estuviese desarrollando un programa como Google Ideas, seguramente sería objeto de una intensa vigilancia crítica[90], pero al parecer Google tiene vía libre en este sentido.

Se trate de una simple compañía o de «más que una simple compañía», las aspiraciones geopolíticas de Google están fuertemente mezcladas con la agenda de política exterior de la superpotencia más grande del mundo. A medida que crece su monopolio de búsqueda y servicios de Internet y se incrementa su ámbito de vigilancia industrial con vistas a alcanzar a la mayor parte de la población mundial, dominando cada vez más el mercado de telefonía móvil y extendiendo su alcance al hemisferio sur, Google se está *convirtiendo* en Internet para mucha gente[91]. Su influencia en las elecciones

y en el comportamiento de la totalidad de los seres humanos se traduce en un poder real para influir en el curso de la historia.

Si el futuro de Internet es realmente Google, mucha gente de todo el mundo —América Latina, Asia oriental y suroriental, el subcontinente indio, Oriente Medio, el África subsahariana, la antigua Unión Soviética e incluso Europa— debería empezar a preocuparse seriamente por buscar una alternativa a la hegemonía cultural, económica y estratégica de Estados Unidos[92].

El imperio de «No seas malo» sigue siendo un imperio.



Para cuando «El imperio de la mente» se convirtió en *The New Digital Age: Reshaping the Future of People, Nations and Business*, publicado en abril de 2013[II], yo ya había solicitado y recibido asilo político del gobierno de Ecuador y me había refugiado en su embajada en Londres, donde llevaba cerca de un año bajo estrecha vigilancia policial, vigilancia que me impedía la salida de la embajada, ya no digamos del Reino Unido[93]. A través de Internet conocí el entusiasmo de la prensa con el libro de Schmidt y Cohen, prensa que ignoraba frívolamente el explícito imperialismo digital del título del libro y la conspicua lista de alabanzas al mismo, incluidas en su contraportada, procedentes de famosos belicistas como Tony Blair, Henry Kissinger, Bill Hayden y Madeleine Albright[94]. Asumí que los argumentos eran poderosos, por lo que me entró curiosidad y convencí a alguien para que pasase de contrabando una copia a través del cordón policial y poder leerlo.

Al principio me quedé totalmente pasmado. Anunciado a bombo y platillo como una visionaria predicción del cambio tecnológico global, el libro era de todo menos una predicción y menos aún visionaria, pues ni siquiera imaginaba un futuro, bueno o malo, sustancialmente distinto del presente. En realidad, el libro era una fusión simplista de la ideología del «fin de la historia» de Fukuyama —pasada de moda desde los años 90— con una mayor velocidad de telefonía móvil, plagada de doctrinas obsoletas de Washington D. C., ortodoxias del departamento de Estado y serviles adulaciones a Henry Kissinger. Su nivel intelectual era muy pobre, incluso degenerado, lo cual no parecía encajar con el perfil de Schmidt, el agudo e ingenioso hombre que había estado en mi sala de estar. Sin embargo, a medida que iba leyendo comencé a ver que el libro no era un intento serio de predecir el futuro, sino una amorosa serenata dedicada por Google a los círculos oficiales de

Washington. Google, floreciente superpotencia digital, se estaba ofreciendo a Washington para ser su visionario geopolítico.

Me quedé esperando las severas críticas que sin duda recibiría el libro, pero estas no llegaron[95]; al contrario, desde la prensa más leída y el sector tecnológico solo llegaban desconcertantes alabanzas. Cada vez más impaciente, decidí redactar yo mismo una reseña, publicada en *The New York Times* el 2 de junio de 2013; en ella decía que «al encontrarse con el mundo grande y malo», Google había «decidido unirse a los poderes tradicionales de Washington, desde el Departamento de Estado hasta la Agencia de Seguridad Nacional». Los apologistas de Google intentaron anular el impacto de mi reseña, tachándola de obra de un paranoico, pero cuatro días después los periódicos de todo el mundo llenaron sus páginas con las filtraciones de Edward Snowden sobre la ASN. El centro de atención fue el escándalo del PRISM, que revelaba todo lo que Eric Schmidt ocultaba cuando en junio de 2011 le pedí que filtrase a WikiLeaks las peticiones de datos del gobierno de Estados Unidos.

Algunas de las declaraciones que se me atribuían en *The New Digital Age* no me sonaban en absoluto a cosas que yo hubiese dicho nunca. Contacté con nuestro departamento de archivo para que me hiciese llegar una copia de la vieja grabación y la volví a escuchar con atención. Por supuesto, Schmidt y Cohen habían tergiversado mis palabras, cosa que, dado el nivel de análisis del libro, tal vez no debería haberme sorprendido. Según iba escuchando la grabación fui apreciando el gran valor de la entrevista, y cómo las circunstancias que rodearon su realización así como las repercusiones posteriores de la misma le habían otorgado una relevancia histórica.

La entrevista contiene descripciones rotundas y nunca vistas de la filosofía subyacente a WikiLeaks, así como de la forma en la que la tecnología afecta a las dinámicas del poder, e incluye conceptos que explican cómo utilizar la tecnología descentralizada para proteger la actividad revolucionaria, ideas que me encantaría ver implementadas. Y en términos de simbolismo, la entrevista prevé dos futuros diferentes y complementarios de Internet: uno, una Internet ubicua en una gobernanza corporativa centralizada; y otro, una Internet vibrante y descentralizada, adecuada para la emancipación de la historia y los seres humanos.

El cuerpo principal de *Cuando Google encontró a WikiLeaks* es la transcripción literal de esta entrevista, aunque con el fin de hacerla más accesible al lector, OR Books y yo hemos revisado conjuntamente el texto y hemos añadido notas explicativas a pie de página. Además de la transcripción,

incluyo también otros escritos que proporcionan el contexto: «La banalidad del ‘No seas malo’» es mi reseña del libro de Schmidt y Cohen publicada en *The New York Times*, con todas sus referencias; y «Líbranos del ‘No seas malo’» es un pequeño panorama sobre la forma en la que WikiLeaks y el contenido de la entrevista quedaron representados (o tergiversados) en *The New Digital Age*. A lo largo de todo este libro existen varias referencias a los diversos intentos del gobierno de Estados Unidos y sus aliados para tomar represalias contra WikiLeaks y sus asociados. Los lectores que no estén familiarizados con estos intentos pueden encontrar al final del libro, en el apartado titulado «Trasfondo de EE. UU. contra WikiLeaks» un pequeño resumen del tema. Una página web creada específicamente al respecto —when.google.met.wikileaks.org— contiene una colección de extractos de comunicados filtrados desde el Departamento de Estado de Estados Unidos y de correos electrónicos internos de Stratfor publicados por WikiLeaks, junto con mucho más material de apoyo a la crítica realizada en estas páginas.

Julian Assange
Mayo de 2014

LA BANALIDAD DEL «NO SEAS MALO»

La reseña de The New Digital Age *fue originalmente publicada en el periódico* The New York Times *el 2 de junio de 2013, poco antes de la aparición de los primeros documentos de Edward Snowden en los diarios* The Guardian *y* The Washington Post[96].

The New Digital Age es un plan de acción del imperialismo tecnocrático sorprendentemente claro y provocativo, elaborado por dos de sus gurús más reconocidos, Eric Schmidt y Jared Cohen, que han creado un nuevo dialecto específicamente para el poder global de Estados Unidos en el siglo XXI. Este dialecto refleja una unión cada vez más estrecha entre el Departamento de Estado y Silicon Valley, representado por el Sr. Schmidt, director ejecutivo de Google, y el Sr. Cohen, exasesor de Condoleezza Rice y Hillary Clinton y actualmente director de Google Ideas.

Los autores se conocieron en 2009 en el Bagdad ocupado, y fue precisamente allí en donde el libro en cuestión fue concebido. Paseando por las ruinas, a ambos les llamó poderosamente la atención el hecho de que la tecnología de consumo estaba transformando una sociedad arrasada por la ocupación militar estadounidense, y llegaron a la conclusión de que la industria tecnológica podría ser un poderoso agente al servicio de la política exterior de Estados Unidos[97].

El libro hace proselitismo del importante papel de la tecnología a la hora de modelar la población y las naciones de todo el mundo a imagen y semejanza de la superpotencia global dominante, quieran o no ser transformadas. La prosa es concisa, los argumentos son contundentes, y la sabiduría es… banal. Pero este no es un libro diseñado para ser leído, sino que se trata de una declaración pensada para fomentar alianzas.

The New Digital Age es, más que cualquier otra cosa, un intento por parte de Google de posicionarse como el principal visionario geopolítico de Estados Unidos, la compañía que puede responder a la pregunta «¿Hacia dónde debería dirigirse Estados Unidos?». No resulta sorprendente que un importante grupo de los más notorios belicistas del mundo se hayan

apresurado a poner su sello de aprobación a esta defensa abierta del poder blando occidental. Los agradecimientos ensalzan la figura de Henry Kissinger, quien junto con Tony Blair y el exdirector de la CIA Michael Hayden alabaron el libro incluso antes de su publicación[98].

En *The New Digital Age* los señores Schmidt y Cohen asumen alegremente lo que podría llamarse «la carga del friki blanco»[III], pues el libro menciona unos pocos ejemplos de convenientes e hipotéticos usuarios de piel oscura: pescadoras congoleñas, diseñadores gráficos en Botsuana, activistas anticorrupción en San Salvador y pastores analfabetos masáis, todos ellos son mencionados como prueba de las propiedades que los teléfonos de Google, conectados a la cadena de información del imperio occidental, tienen para el progreso.

Los autores ofrecen una versión expertamente banalizada del mundo del mañana: los aparatos electrónicos de las próximas décadas serán muy parecidos a los actuales, solo que «molarán» más. El «progreso» vendrá determinado por el inexorable avance de la tecnología estadounidense por toda la superficie de la tierra. Actualmente se activan cada día más de un millón de nuevos dispositivos móviles gestionados por Google[99], por lo que en breve la compañía se interpondrá en las comunicaciones de todos y cada uno de los seres humanos que no se encuentren en China (estos chinos…), y con ella el gobierno de Estados Unidos. Los productos cada vez son más maravillosos; los profesionales jóvenes y urbanitas duermen, trabajan y compran de forma cada vez más fácil y cómoda; la democracia se ve insidiosamente subvertida por las tecnologías de vigilancia y control; y nuestro actual orden mundial de dominación, intimidación y opresión sistemáticas sigue sin verse siquiera mencionado, afectado o ligeramente perturbado.

Los autores se muestran resentidos por el triunfo egipcio de 2011, y ridiculizan desdeñosamente a la juventud egipcia, afirmando que «la mezcla de activismo y arrogancia en los jóvenes es universal»[100]. Los movimientos sociales apoyados por el mundo digital conducen a revoluciones que serán «más fáciles de comenzar» pero «más difíciles de terminar»[101]. Debido a la ausencia de líderes fuertes, el resultado serán gobiernos en coalición que acabarán convirtiéndose en autocracias, o al menos es lo que dijo el Sr. Kissinger a los autores[102], que a su vez afirman que ya no habrá «más primaveras» (pero China está contra las cuerdas)[103].

Los autores fantasean sobre el futuro de los grupos revolucionarios «bien provistos de recursos». Una nueva «cosecha de consultores» usará «los datos

para construir y perfeccionar una figura política»[104].

«Sus» discursos (el futuro no es tan diferente) y comunicados escritos se alimentarán de «complejos *softwares* de extracción de datos y análisis de tendencias» mientras «se mapean sus funciones cerebrales», y se emplearán otros «sofisticados diagnósticos para evaluar las partes más débiles de su repertorio político»[105].

El libro se hace eco de los tabúes y obsesiones institucionales del Departamento de Estado, al tiempo que, significativamente, evita criticar a Israel y a Arabia Saudí. De forma bastante sorprendente, afirma que el movimiento de soberanía latinoamericano, que durante los últimos treinta años ha liberado a tantas personas de plutocracias y dictaduras apoyadas por Estados Unidos, en realidad nunca ha existido; al hacer referencia en su lugar a los «envejecidos líderes» de la región, el libro refleja que no puede ver a América Latina a causa de Cuba[106]. Y, por supuesto, los autores, de forma muy teatral, se muestran inquietos por los hombres del saco favoritos de Washington: Corea del Norte e Irán[107].

Google, que comenzó siendo una expresión de la cultura independiente de estudiantes de posgrado californianos —una cultura decente, humana y alegre—, al encontrarse con el mundo grande y malo se ha ido uniendo progresivamente a los poderes tradicionales de Washington, desde el Departamento de Estado hasta la Agencia de Seguridad Nacional.

El terrorismo, a pesar de suponer apenas una fracción infinitesimal de las muertes violentas a nivel mundial, es una de las marcas favoritas de los círculos políticos de Estados Unidos. Este es un fetichismo que también debe ser satisfecho, y por tanto «El futuro del terrorismo» tiene su propio capítulo aparte[108], en el que nos enteramos de que el futuro del terrorismo es el «ciberterrorismo»[109]. Este capítulo constituye toda una sesión de estremecedor alarmismo, incluyendo un hipotético escenario de película de desastres que deja sin aliento: ciberterroristas se hacen con el control del sistema de navegación aérea estadounidense y provocan innumerables choques de aviones contra edificios emblemáticos, desconectan redes de alimentación eléctrica y hasta lanzan bombas nucleares[110]. Seguidamente, los autores pintan con el mismo pincel a los activistas que organizan encuentros y debates digitales[111].

Mi perspectiva es muy diferente: el avance de la tecnología de la información encarnado por Google anuncia la muerte de la privacidad para la mayoría de las personas y reconduce al mundo hacia el autoritarismo. Esta premisa es la tesis principal de mi libro *Cypherpunks: la libertad y el futuro*

de Internet[112]. Sin embargo, mientras que los Sres. Schmidt y Cohen nos dicen que en las «autocracias represivas» la muerte de la privacidad ayudará a sus gobiernos a «acosar a sus ciudadanos», también dicen que los gobiernos de las democracias «abiertas» lo considerarán como «un regalo» que les permitirá «responder de la mejor forma posible a las preocupaciones de sus ciudadanos y sus clientes»[113]. En realidad, la erosión de la privacidad individual en Occidente y la consiguiente centralización del poder hacen que los abusos resulten inevitables, por lo que las sociedades «buenas» cada vez se parecen más a las «malas».

La sección sobre «autocracias represoras» describe con desaprobación varias medidas de vigilancia represiva: legislación para insertar accesos ocultos al *software* comercial para espiar a los ciudadanos, control de las redes sociales y almacenamiento de datos confidenciales de poblaciones enteras[114]. Todas estas medidas ya están firmemente implantadas en Estados Unidos, y de hecho algunas de ellas —como el requisito de que todo perfil en la red social esté asociado a un nombre real— fueron propuestas y abanderadas por el propio Google[115].

La escritura está en la pared[IV], pero los autores se niegan a verla. Tomaron prestada de William Dobson la idea de que en una autocracia los medios de comunicación oficiales «permiten una prensa no afín al régimen siempre que los opositores entiendan dónde están sus límites, aunque no estén escritos»[116], pero estas tendencias están comenzando a emerger en Estados Unidos. Nadie duda de los escalofriantes efectos de las investigaciones practicadas a Associated Press y a James Rosen, de la Fox[117], pero ha habido muy poca investigación sobre el papel de Google en relación con la citación a declarar de Rosen.

Yo mismo he tenido experiencias personales con estas tendencias.

En marzo de 2013, el Departamento de Justicia admitió que se había pasado los últimos tres años investigando criminalmente a WikiLeaks, y algunos testimonios judiciales afirman que entre sus objetivos se encuentran «los fundadores, propietarios o gerentes de WikiLeaks»[118]. Una supuesta fuente, Bradley Manning, se enfrenta a un juicio de doce semanas a contar desde mañana mismo (3 de junio de 2013), en el que se espera que hasta veinticuatro testigos de cargo presten declaración en secreto[119].

The New Digital Age es una obra siniestramente trascendente en la que ninguno de sus dos autores tiene la capacidad para ver, y mucho menos para expresar, el diabólico engendro centralizador que están creando. «La

tecnología y la ciberseguridad», nos dicen, «es al siglo XXI lo que Lockheed Martin fue al siglo XX»[120].

Sin siquiera saber muy bien cómo, lo que han logrado los autores es actualizar e implementar la profecía de George Orwell. Si se desea tener una visión del futuro, basta con imaginar una legión de rostros inexpresivos tras las gafas Google Glass patrocinadas por Washington, de aquí a la eternidad. Los fanáticos del culto a la tecnología consumista encontrarán en todo esto muy poca inspiración para actuar, pero este libro es de lectura obligada para todo aquel atrapado en la pelea por el futuro, aunque solo sea por un simple imperativo: conoce a tu enemigo.

ELLINGHAM HALL, 23 DE JUNIO DE 2011

Julian: Julian Assange Fundador y redactor jefe de WikiLeaks.

Eric: Eric Schmidt Director ejecutivo de Google; coautor de *The New Digital Age*; miembro del Consejo Asesor sobre Ciencia y Tecnología del presidente Obama; miembro del Consejo de Relaciones Internacionales[121].

Jared: Jared Cohen Director de Google Ideas; coautor de *The New Digital Age*; exmiembro del equipo de planificación política del Departamento de Estado y consejero de Condoleezza Rice y Hillary Clinton; miembro del consejo asesor del director del Centro Nacional de Antiterrorismo; miembro senior del Consejo de Relaciones Internacionales; cofundador de Movements.org[122].

Lisa: Lisa Shields Vicepresidenta, directora de comunicación global y portavoz del Consejo de Relaciones Internacionales; exproductora de televisión de los programas *Good Morning America* y *Primetime* Live[123].

Scott: Scott Malcomson Director de comunicaciones de International Crisis Group; editor de *The New Digital Age*; redactor jefe de discursos para Susan Rice en el Departamento de Estado de Estados Unidos en 2011-2012; miembro vitalicio del Consejo de Relaciones Internacionales[124].

La siguiente conversación fue grabada en casa de Vaughan Smith, en Norfolk, Inglaterra, donde viví bajo arresto domiciliario en el año 2011. Como condición para librarme provisionalmente de la cárcel, durante todo el tiempo que estuve en Norfolk tuve que llevar un dispositivo localizador en el tobillo, y se instalaron tres antenas repetidoras en la casa que transmitían la señal, de forma que el gobierno británico estaba al tanto de todos mis movimientos.

La entrevista comenzó en la cocina mientras comíamos, continuó brevemente en la sala de estar y terminó durante un paseo por los alrededores

de la casa, paseo que tuvimos que acortar debido a la aproximación de una tormenta.

Algunas de mis contribuciones han sido ligeramente revisadas en aras de la brevedad y la facilidad de lectura, pero no se ha alterado nada significativo. No he modificado absolutamente nada de las palabras de los demás implicados, pues no contaba con su permiso (después de todo, no me gustaría tergiversarlas por accidente). Únicamente se han realizado pequeños cambios en el orden de las intervenciones con el fin de mejorar el flujo de la conversación.

En la página web de WikiLeaks puede escucharse la grabación íntegra de tres horas, como prueba de la integridad de la transcripción[125].

DE LOS QUE VEN A LOS QUE ACTÚAN

[Comienzo de la grabación]

Eric Schmidt: Bueno, ¿queréis que empecemos a comer?

Julian Assange: Podemos hacer ambas cosas

Eric: Claro, ¿por qué no?

Julian: Bien, estamos a 23 de junio. Esta es una grabación entre Julian Assange, Eric Schmidt, y…

Lisa Shields: Lisa Shields

Julian: Lisa Shields. Para ser utilizada por Eric Schmidt en un libro, cuya publicación está previsto que la realice Knopf en octubre de 2012[126]. Se me ha garantizado que tendré acceso a la transcripción y que podré modificarla para mejorar la precisión y la claridad[127].

Eric: Estamos de acuerdo

Lisa: Estamos de acuerdo

Eric: ¿Podemos empezar? Me gustaría hablar un poco sobre Thor. Bien, en cierto modo, toda la red de la Marina…

Julian: ¿Thor o Tor?

Eric: Si, eso es, quería decir Tor[128]

Julian: Y Odín también[129]

Eric: Está bien, está bien; Tor y la red de la Marina. No entiendo realmente cómo funcionaba todo eso. La razón por la que lo menciono es que ante todo estoy interesado en lo que ocurre con la tecnología a medida que evoluciona. Por tanto, diría que el problema es que cuando se está tratando de obtener información se necesita tener garantías de anonimato por parte del emisor de la misma, el destinatario necesita tener un canal seguro, tiene que poder reproducirla. […] Lo que me gustaría que hicieras[V] es hablar un poco sobre esa arquitectura, lo que hicisteis en WikiLeaks a nivel técnico, las innovaciones técnicas que se necesitaron y también lo que le ocurre[130]. ¿Cómo evoluciona? La tecnología siempre está evolucionando.

Julian: Antes de nada, déjame que te explique un poco el marco de lo que hago. Yo había visto que había muchas cosas que ocurrían en el mundo que eran injustas, y mi deseo era que hubiese menos actos injustos y más actos justos. Alguien me puede preguntar: «¿Cuáles son tus axiomas filosóficos en todo esto?», y yo le respondo: «No necesito considerarlos siquiera. Esto es solo mi forma de ser, y para mí es un axioma simplemente porque lo es». Esto evita meterse en discusiones filosóficas que no ayudan a nadie acerca de la razón por la que hago algo. Lo hago, y punto.

Al reflexionar sobre la forma en la que se cometen actos injustos, qué tiende a promover tales actos, y qué promueve los actos justos, me di cuenta de que los seres humanos son básicamente invariables, es decir, que sus inclinaciones y su temperamento biológico no han cambiado mucho desde hace miles de años. Por tanto, el único campo de acción que me quedaba era: ¿qué tienen y qué saben los humanos? Lo que tienen —de qué recursos disponen, cuánta energía pueden utilizar, qué reservas de alimentos poseen, etc.— es algo bastante difícil de modificar, pero lo que saben puede ser alterado de forma no lineal porque cuando una persona proporciona información a otra, esta puede transmitirla a otra, esta a otra, y así sucesivamente, de manera no lineal[131]. De este modo, se puede llegar a muchas personas con una cantidad de información pequeña, por lo que se puede cambiar el comportamiento de mucha gente con poca información. La cuestión que esto plantea es: ¿Qué tipo de información incentiva los comportamientos justos y desincentiva los injustos?

En el mundo hay personas que observan diferentes aspectos de lo que les está pasando a nivel local; hay otras personas que reciben información de cosas

que no les han ocurrido a ellos directamente; y en el medio se sitúan las personas que están involucradas en el desplazamiento de la información desde los observadores directos a los que posteriormente actuarán con base en esa información. Tenemos, por tanto, tres problemas diferentes relacionados entre sí.

Yo era consciente de la dificultad de extraer las observaciones y ubicarlas de manera eficiente en un sistema de distribución que, a su vez hiciese llegar esta información a aquellas personas que quieran actuar en función de ella. Se puede argumentar que compañías como Google, por ejemplo, se dedican a la parte de «intermediación», es decir, a trasladar la información desde la gente que la tiene a la gente que la quiere. El problema que vi fue que, en aquellos casos en los que se tratase de información que los gobiernos se sintiesen inclinados a censurar, el primer paso se vería interrumpido, y a menudo el último también.

Podemos considerar todo este proceso como justicia producida por el cuarto poder[132]. Esta descripción, derivada en parte de mis experiencias con la mecánica cuántica, atañe al flujo de determinados tipos de información que en última instancia podrían provocar algún tipo de cambio. En mi opinión, el principal cuello de botella se encontraba en la obtención de información que llevase a producir cambios que pudiesen considerarse como justos. En el contexto del cuarto poder, las personas que obtienen información son las fuentes; las que trabajan con esa información y la distribuyen son los periodistas y los editores; y las que actúan sobre ella básicamente es toda la población. Este es el esquema general, pero en esencia se reduce a cómo diseñar un sistema práctico que resuelva este problema, y no solo un sistema técnico, sino un sistema global. WikiLeaks era, y aún es, un intento —aún muy joven— de crear un sistema global.

En el frente técnico, nuestro primer prototipo fue diseñado para una situación realmente adversa en la que la publicación resultase extremadamente difícil y nuestro único medio de defensa efectivo fuese el anonimato, en el que la localización de las fuentes fuese extremadamente difícil (como lo sigue siendo en el sector de seguridad nacional), y en el que tuviésemos un equipo muy pequeño y de absoluta confianza.

Eric: Entonces, en este caso ¿al decir publicación te refieres a la propia página web y a la puesta a disposición del material al público?

Julian: Sí, a la puesta a disposición. A eso me refiero con publicación.

Eric: ¿El primer paso era entonces hacer esto correctamente?

Julian: Para mí estaba muy claro que en todo el mundo la publicación constituye un problema, sea por autocensura o por censura pública.

Eric: Disculpa, ¿eso se debe al miedo a represalias por parte del gobierno? ¿O a todo tipo de causas?

Julian: Sobre todo es autocensura. De hecho, yo diría que históricamente la forma más importante de censura ha sido la económica, aquellos casos en los que sencillamente no es rentable publicar algo porque no existe mercado para ello. A menudo describo la censura como una pirámide. En la parte más alta de esta pirámide están los asesinatos de periodistas y editores. En un nivel más abajo se encuentran los ataques legales a periodistas y editores. Un ataque legal es simplemente un uso progresivo de una fuerza coercitiva, que no implica necesariamente el asesinato pero que puede tener como consecuencia la encarcelación o la confiscación de propiedades. Está claro que el volumen de una pirámide se incrementa a medida que se desciende por ella desde la cúspide, y en este ejemplo concreto esto significa que el número de actos de censura también se incrementa a medida que se desciende.

Hay muy poca gente que sea asesinada, y algunos más que sean víctimas de ataques legales públicos, sean individuos o corporaciones. Más abajo, en el siguiente nivel, existe una tremenda cantidad de autocensura, que ocurre en parte porque mucha gente no desea subir a los niveles más altos de la pirámide: no están dispuestos a correr el riesgo de ser blanco de fuerzas coercitivas, y por supuesto no desean ser asesinados. Esto desanima a muchas personas a comportarse de determinada forma. Por otro lado, también hay otras formas de autocensura motivadas por la preocupación de perder acuerdos comerciales o ascensos profesionales, y estas son aún más importantes porque están todavía más abajo en la pirámide. Por último, en la misma base —que posee el volumen más grande— están todas aquellas personas que no saben leer, que no tienen acceso a publicaciones o comunicaciones rápidas, o que no existe una industria rentable que se la proporcione[133].

Tomamos la decisión de centrarnos en los dos niveles superiores de esta pirámide de censura: amenazas de violencia inmediata y amenazas de violencia en diferido, ejercidas por el sistema legal. Los casos de estos niveles pueden ser los más fáciles pero también pueden ser los más difíciles. Pueden ser los más fáciles porque está muy claro cuándo las cosas están siendo

censuradas y cuándo no, y también porque el volumen de censura es relativamente pequeño, incluso si la importancia de cada acontecimiento puede ser muy grande.

Al principio WikiLeaks no tuvo demasiados amigos. Aunque yo tenía por supuesto algunas conexiones políticas previas de mis otras actividades, en realidad no teníamos aliados políticos significativos y tampoco teníamos una audiencia global pendiente de lo que hacíamos. Por ello, llegamos a la conclusión de que necesitábamos un sistema de publicación en el que nuestra única defensa fuese el anonimato. No teníamos protección financiera; no teníamos protección legal; y no teníamos protección política. La única protección que teníamos era la puramente técnica.

Esto implicaba crear un sistema que tuviese un frente distribuido[134] con muchos nombres de dominios y una gran capacidad para cambiar esos nombres rápidamente[135], un sistema de memoria caché[136], y, en la parte trasera, un pasadizo secreto a través de la red de Tor hasta los servidores ocultos[137].

Eric: Quisiera hablar un poco sobre esto. Entonces, podéis cambiar muy rápidamente de DNS, de nombre de dominio, etcétera[138]. ¿Os servís de los pasadizos para comunicaros entre estas réplicas? ¿O son solo para distribución?

Julian: Teníamos nodos frontales sacrificables[139], muy fáciles y rápidos de poner en marcha, aunque los ubicábamos en jurisdicciones relativamente hospitalarias como Suecia[140]. Estos nodos frontales eran muy rápidos porque había que dar muy pocos saltos entre ellos y las personas que los leían[141]. Esta es una lección importante que yo había aprendido de mi experiencia: ser un tanque Sherman no es siempre una ventaja, puesto que tu maniobrabilidad y tu velocidad no son demasiado elevadas. Buena parte de la protección para los encargados de publicar es hacerlo lo más rápido posible, pues si publicas con rapidez y la gente lee pronto lo que publicas, el incentivo de que alguien pueda ir a por ti en relación con esa información determinada es casi cero, puesto que ya llegarían tarde. Es posible, no obstante, que tengan incentivos para ir a por ti para darte un escarmiento y que tu organización no vuelva a desafiar su autoridad en el futuro, o para que este escarmiento sirva de advertencia a otros que pudiesen tener la intención de desafiar tal autoridad.

Eric: Así pues, insisto para fijar el argumento, os preocupaba que los gobiernos o quien fuese atacase los frentes de la página bien mediante ataques

de denegación de servicios[142] o mediante ataques de bloqueo, básicamente aplicando filtros[143], como se suele hacer. Entonces, un aspecto importante de todo esto era estar siempre disponible.

Julian: Siempre disponibles de una forma u otra. Esta es una batalla que hemos ganado en su mayor parte, pero no del todo. En pocas semanas, el gobierno chino nos añadió a su lista de páginas prohibidas. Pero teníamos cientos de nombres de dominio de varios tipos registrados en servidores DNS realmente grandes, de forma que si se producía un filtrado nivel DNS-IP[144] se filtraban también 500 000 dominios junto con el nuestro, y ello provocaría una violenta reacción política que les haría echarse atrás. Sin embargo, el filtrado basado en el DNS nos siguió afectando en China, ya que los nombres más comunes —los más parecidos a «WikiLeaks», el nombre más fácilmente transmitido entre las personas— están todos filtrados por el gobierno chino.

Eric: Por supuesto

Julian: Cualquier dominio que incluya «WikiLeaks» en alguna parte, sea donde sea, es filtrado. Esto significa que tiene que haber una variante que aún no han descubierto, pero esta variante tiene que ser lo suficientemente conocida como para que la gente se dirija a ella. Es un círculo vicioso.

Eric: Eso es un problema estructural asociado a los nombres de Internet, pero los chinos podían limitarse a filtrar vuestros contenidos[145].

Julian: Bueno, los HTTPS funcionaron cerca de un año y medio[146].

Eric: Ya.

[Ruido de fondo. Jared Cohen y Scott Malcomson entran en este momento en la habitación]

Julian: De hecho, funcionaron bastante bien. Y el cambio de IP también funcionó[147]. El sistema de filtrado chino de Internet era bastante barroco. Lo han mejorado. A veces hacen las cosas manualmente y a veces de forma automática, añadiendo IP a la lista de nombres de dominio. Tuvimos una batalla bastante interesante en la que nos dimos cuenta de que estaban buscando nuestras IP, y vimos que estas peticiones procedían de cierto bloque de direcciones IP en China[148]. Cada vez que veíamos esto nos limitábamos a regresar de otra forma[149].

Eric: Ja ja ja ja ja. Muy listos. Ja ja ja ja ja.

Julian: Pensé: ¡vamos a regresar con las IP del Ministerio de Seguridad Pública![150]

Eric: Eso es muy gracioso. Este es Jared Cohen, por cierto.

Jared Cohen: Hola, siento llegar tarde. El vuelo se retrasó.

Julian: Encantado de conocerte.

Eric: Volabas con United, ¿no?

Jared: No, con Delta. ¡Pero nunca más!

Eric: Sí, muy típico de Delta.

Julian: ¿Larry?

Jared: Jared.

Julian: ¡Jared, Jared!

Eric: Y este es Scott.

Scott Malcomson: ¡Un placer!

Eric: Scott es nuestro editor.

Scott: Perdón, llegamos una hora y media tarde.

Julian: ¡No pasa nada! ¡Hace un día precioso para conducir!

Eric: En realidad, hemos tenido un tiempo estupendo.

Scott: Claro, claro, claro.

Lisa: ¡Julian ha sido muy amable, porque no hemos traído grabadora!

Eric: Ja ja ja ja ja.

Lisa: Hay que admitir que es bastante embarazoso solicitar una entrevista y tener que pedirle prestada la grabadora al propio entrevistado.

Julian: Un amigo mío hizo una entrevista en Fiji durante el golpe de estado del general Rabuka, y el lugarteniente del general le confesó en plena grabación que la CIA les había pagado por llevar a cabo el golpe[151].

Eric: ¡Guau!

Julian: Mi amigo volvió pensando: «¡Sí! ¡Tengo la noticia de la década!» Y luego resultó que la cinta no había grabado. Por eso ahora tengo muchas de estas ¡Siempre hay que tener muchas!

[Risas]

Eric: Siempre, siempre hay que tener la tuya propia.

Para información de Scott y Jared, decir que hemos pasado un buen rato charlando sobre Google y sobre lo que tenemos entre manos. He presentado a Lisa. No he logrado explicar como es debido lo brillante que es el libro en el que estamos trabajando, y Lisa me ha ayudado. Julian se ha mostrado conforme con esta ayuda. Hemos acordado hablar sobre tecnología y sus implicaciones. El trato ha sido grabar todo esto para el libro, grabación que transcribiremos para que Julian tenga la oportunidad de modificar, alargar o mejorar su claridad, y todo me ha parecido realmente razonable.

Acabamos de empezar. Hemos hablado un poquito sobre los principios generales que Julian ha articulado, y ahora mismo estaba comenzando a hablar sobre la estructura: por qué WikiLeaks se ha diseñado de la forma en que lo ha hecho. Y un resumen aproximado es que la principal preocupación que tenía a la hora de diseñar la página era que cuando se observase a los gobiernos se supiese las cosas que hacen: asesinar periodistas, encarcelarles, todo eso. Su idea era que para enfrentarse al problema era necesario crear un sistema muy, muy difícil de bloquear. Por tanto, la explicación no técnica de lo que hizo es que creó un sistema en el que si se llevan a cabo las acciones habituales para bloquearlo, simplemente aparece de otra forma: cambia su nombre y crea réplicas.

EL NOMBRE DE LAS COSAS

Julian: El nombre de las cosas es muy importante. El nombre que se le pone al trabajo intelectual del ser humano y a todo nuestro legado intelectual es posiblemente la labor humana más importante. Todos tenemos palabras para diferentes objetos, como «tomate»; usamos una palabra simple, «tomate», en lugar de describir cada pequeño detalle de un maldito tomate[152]. Como lleva demasiado tiempo describir con precisión el aspecto de un tomate, nos servimos de una abstracción para poder pensar en él y hablar de él. Y lo mismo hacemos al usar URL[153], que a menudo se utiliza como una abreviación de un conjunto de conocimientos intelectuales humanos. Nuestras civilizaciones están construidas, aparte de por ladrillos, por conocimientos

intelectuales. Pues bien, actualmente tenemos un sistema de URL cuya estructura, con la que estamos construyendo nuestra civilización, está hecha de plastilina de la peor calidad, y eso es un gran problema.

Eric: Y se podría decir que es preciso desarrollar una estructura de nombres distinta, una que permitiese una mejor…

Julian: Pienso que existe una enorme confusión, un desgaste de la idea que se tiene actualmente de las URL.

Eric: Sí. Totalmente de acuerdo.

Julian: Por un lado, tenemos los servicios dinámicos en directo y las organizaciones que gestionan estos servicios, lo que conlleva una jerarquía y un sistema de control, sea este ejercido por una organización, un gobierno o cualquier otro grupo de control. Y por otro, tenemos los conceptos intelectuales humanos que pueden ser completamente independientes de cualquier sistema de control humano, que están ahí fuera en el terreno de lo platónico**[154]**; uno debería referirse a ellos con base en su contenido intelectual intrínseco, y no por la forma en que dependan de una organización. Pienso que esto tendría que ser un paso adelante inevitable y muy importante.

La primera vez que me di cuenta de que esto era un problema fue al tratar con un hombre llamado Nadhmi Auchi**[155]**. Hace unos años, una de las grandes revistas de negocios le situó en el quinto lugar de la lista de hombres más ricos de Reino Unido. Nacido en Irak, inicialmente trabajó para el Ministerio del Petróleo iraquí, y se hizo rico antes de trasladarse a Reino Unido a comienzos de los años 80. Según la prensa italiana, estuvo involucrado en numerosos negocios de armamento. Posee más de cien compañías gestionadas desde su *holding* en Luxemburgo y algunas más que descubrimos en Panamá a nombre de su mujer. Logró infiltrarse hasta tal punto en el círculo político laborista británico que en la celebración en Londres del vigésimo aniversario de su actividad comercial se le regaló un cuadro firmado por los 130 ministros y miembros del Parlamento, incluyendo el primer ministro Tony Blair.

Nadhmi Auchi era uno de los financieros de Tony Rezko, que a su vez era recaudador de fondos en Chicago para Rod Blagojevich, exgobernador del estado de Illinois. Tanto Rezko como Blagojevich fueron más tarde condenados por corrupción. Tony Rezko también fue el intermediario que ayudó a Barack Obama a comprar parte de su residencia habitual.

Estos son detalles, pero significativos. Durante las primarias presidenciales de 2008, Barack Obama comenzó lógicamente a atraer mucho la atención de la prensa estadounidense, que comprobó la lista de sus patrocinadores, descubriendo primero a Tony Rezko y volviendo después la vista hacia Nadhmi Auchi. Al saberse observado, Auchi contrató los servicios de Carter-Ruck, una firma londinense de pésima reputación, especialista en pleitos por difamación y calumnias, de cuyo fundador, Peter Carter-Ruck, se había llegado a decir que había hecho por la libertad de expresión lo que el estrangulador de Boston hizo por los vendedores ambulantes[156]. La firma comenzó su labor escribiendo cartas a todos los periódicos de Londres que tenían registros de su extradición a Francia en 2003 y de su condena por fraude en el escándalo del Elf Aquitaine, en el que estuvo implicado por canalizar comisiones ilegales sobre la venta de refinerías de petróleo de Kuwait durante la ocupación de este país en la primera guerra del Golfo[157].

Poco después, *The Guardian* eliminó seis de sus artículos de 2003 sin decir una palabra a nadie, artículos que habían estado en el archivo online del periódico durante cinco años; si se visitan sus URL no se ve «página eliminada por amenazas legales», se ve solo «página no encontrada». Lo mismo pasó con un artículo de *The Telegraph*, otros de algunas publicaciones y blogs de Estados Unidos, etcétera. Importantes bits de la historia reciente, relevantes para la campaña electoral estadounidense que estaba teniendo lugar en ese mismo momento, fueron eliminados de los archivos[158]. Además, también fueron eliminados del índice de artículos de *The Guardian*, por lo que a pesar de que existen ejemplares impresos del periódico y se puede ir a alguna hemeroteca para consultar los artículos, ¿cómo se sabría que están ahí? No figuran en ningún índice. No solo ya no existen, sino que ahora nunca existieron. Es la implementación moderna de la vieja máxima de Orwell: «Quien controla el pasado, controla el futuro; quien controla el presente, controla el pasado», porque todos los hechos documentados del pasado están almacenados físicamente en el presente[159].

La cuestión de la preservación de archivos políticamente destacados cuando son objeto de ataques es la premisa central de la labor de WikiLeaks, porque ese es nuestro objetivo. Nos interesa proteger aquellos bits[160] que alguien intenta suprimir porque sospechamos, a menudo con razón, que si dedican esfuerzo económico a su supresión es porque consideran que van a provocar algún cambio.

Scott: Entonces, ¿lo que buscáis parar determinar el valor son pruebas de supresión?

Julian: Sí […] no exactamente, pero es una buena…

Scott: Entonces, dime qué es exactamente.

Julian: Bueno, no siempre se acierta. Pero es muy sugestivo…

Scott: ¡No es perfecta!

Julian: No, no es algo perfecto, pero es muy sugerente que la gente que mejor conoce la información —la gente que la redactó— dedique medios económicos a impedir el acceso a un archivo histórico, para que el público no pueda leerlo. ¿Por qué tantas molestias para hacer eso? Es más eficiente simplemente dejar que todo el mundo tenga acceso: no solo no hay que emplear recursos para custodiarlo, sino que, gracias a todas las consecuencias positivas no previstas de la circulación de la información, también es más eficiente para tu organización. Por tanto, nos centramos en esta información suprimida de forma selectiva en las propias organizaciones, y con mucha frecuencia, si se trata de un grupo poderoso, tan pronto como alguien trata de publicarla se detectan intentos para eliminarla inmediatamente después de la publicación.

Eric: Me gustaría saber un poco más sobre la tecnología. Entonces, en esta estructura, básicamente se pueden crear nuevas portadas muy rápidamente y almacenar réplicas que luego se distribuyen. Una de las dudas que me surgen es: ¿Cómo se decide qué ISP utilizar?[161]

Julian: Muy buena pregunta.

Eric: Si, en realidad se trata de una serie de cuestiones bastante complicada.

Julian: Te pondré un ejemplo de cómo no se deben escoger. En una ocasión supimos de un caso en las Islas Turcas y Caicos, donde existía un grupo, pequeño pero fantástico, llamado *TCI Journal* (*Turks and Caicos Islands Journal*)[162]. Este grupo, que está formado por activistas locales, son personas con mentalidad ecologista que vieron como empezaban a llegar promotores que se las arreglaban para adquirir terrenos muy baratos en nombre de la Corona y empezar a construir rascacielos[163], y empezaron a hacer una campaña en favor de una buena ordenación territorial encaminada a parar los pies a todos esos promotores.

Es un clásico ejemplo de buen uso de Internet: la publicación barata implica que tengamos muchos más tipos de editores, incluidos aquellos que se autofinancian. La gente puede publicar simplemente por razones ideológicas o altruistas, porque los costes del altruismo a la hora de hacer llegar las ideas son lo suficientemente bajos como para que merezca la pena. Pues bien, los promotores encontraron rápidamente la forma de expulsar de los servidores a los activistas de las Islas. Entonces los trasladaron a la India, pero el promotor que se había ocupado de echarlos de los servidores de las Islas contrató abogados en Londres, que a su vez subcontrataron abogados en India, que se encargaron de anular también sus servidores situados en el ISP local. Seguidamente los activistas los trasladaron a Malasia, pero ocurrió exactamente lo mismo: tan pronto como empezaron a llegar comunicados legales al ISP local, los activistas dejaron de ser rentables para el ISP. Por último, se trasladaron a Estados Unidos, pero su ISP estadounidense rehusó directamente aceptarles, por lo que escogieron otro que era un poco mejor. A causa de las amenazas, los editores eran anónimos; aunque los columnistas a menudo no lo eran, la parte responsable de la publicación sí. Sin embargo, cuando los abogados de los promotores se percataron de que los activistas utilizaban una cuenta de correo de Gmail, presentaron entonces una demanda en California, y como consecuencia los juzgados comenzaron a emitir citaciones judiciales, incluso contra el propio Gmail. El resultado fue que Google comunicó al *TCI Journal* que tenían que trasladarse a California para defenderse y que si no lo hacían tendría que cancelar el servicio de la cuenta de correo.

Se trataba de un grupo muy pequeño de las Islas Turcas y Caicos que intentaba detener la corrupción en su país, enfrentándose a promotores de enormes recursos. ¿Cómo podían luchar contra una citación que formaba parte de una demanda fraudulenta por supuestas injurias? Por supuesto, no podían. Pero logramos conseguirles unos abogados, y casualmente el código estatutario de California contiene una disposición que legisla esa situación concreta, en la que alguien publica algo y otros emiten una citación para intentar averiguar su identidad. Según este código, tal cosa no se puede hacer, y quien lo haga debe pagar una multa. Es una cláusula estupenda que alguien había introducido en el código. Google no mandó ni un solo abogado para ayudarles.

Esto es un ejemplo de lo que ocurre cuando eres un grupo bastante brillante —tenían un técnico indio muy bueno y brillantes estrategas políticos— y te

propones acabar con la corrupción en tu país utilizando Internet como mecanismo de publicación. ¿Qué ocurre? ¿Que te persiguen literalmente por todo el mundo? Este grupo tuvo la suerte de que tenía los suficientes recursos como para sobrevivir a esta persecución, y que acabaron encontrando algunos amigos y una buena defensa legal.

Para nosotros era una cuestión de averiguar que ISP habían soportado la presión. Como yo he estado implicado en política, tecnología y anticensura durante mucho tiempo, conocía a algunos de los jugadores. Contábamos con ISP en los que ya habíamos infiltrado nuestra ideología, donde teníamos amigos que sabíamos que lucharían en nuestro bando si fuese necesario, y sabíamos que había una buena posibilidad de que si se emitían citaciones nos íbamos a enterar pronto, incluso en el caso de que estuviesen protegidas por secreto de sumario.

¿Podría alguien que no está en este mundillo hacer algo así? No sería fácil. Se puede echar un vistazo a los ISP que actualmente utiliza WikiLeaks, o que Pirate Bay o cualquier otro grupo ha utilizado, y se verá que sufren tremendos ataques[164]. A menudo los que más lo sufren son los ISP pequeños. En Suecia existe un pequeño ISP llamado PRQ, fundado por Gottfrid, apodado anakata, uno de los cerebros técnicos de Pirate Bay[165], que ha desarrollado un nicho en la industria en colaboración con Bahnhof, otro ISP sueco más grande, y tratan con publicadores refugiados, literalmente: publican material de refugiados[166].

Además de a WikiLeaks, PRQ da servicio a la Asociación de Propietarios de Viviendas de Estados Unidos, que tuvo que huir de los promotores inmobiliarios estadounidenses; también al Centro Kavkaz, un centro de noticias ubicado en el Cáucaso que sufre constantes ataques de los rusos (de hecho, PRQ ha sido registrado varias veces por un gobierno sueco presionado por el ruso); y al Instituto Rick A. Ross para el Estudio de Cultos Peligrosos, un grupo estadounidense que se había visto obligado a abandonar Estados Unidos por una demanda de la Iglesia de la Cienciología[167].

Otro ejemplo es *Malasia Today*, gestionado por un tipo estupendo llamado Raja Petra, que tiene sobre su cabeza dos órdenes de arresto en Malasia. Por ello, huyó a Londres, pero sus servidores no pueden sobrevivir allí, por lo que están ubicados en Singapur y en Estados Unidos[168].

Eric: Sin embargo [*inaudible*] hay muchas otras páginas que participan en esto.

Julian: Sí, unas mil cuatrocientas; tenemos espejos voluntarios[169].

Eric: ¿Entonces son páginas espejo voluntarias?

Julian: Son ellas las que evalúan los riesgos que asumen. No sabemos nada de ellas. No podemos garantizar que todas ellas sean de fiar, pero su número se incrementa constantemente.

Eric: Según la prensa, alguna vez has dicho que existe un volumen de información codificado y distribuido mucho más grande del que publicáis. ¿Se distribuye en este tipo de sitios?

Julian: No, nosotros distribuimos abiertamente copias de seguridad codificadas de los materiales que consideramos altamente sensibles y que tenemos intención de publicar el año que viene[170].

Eric: Entiendo.

Julian: No para tener un «dispositivo termonuclear» que podamos usar contra nuestros oponentes, tal y como han dicho algunas personas, sino más bien para minimizar la posibilidad de que tal material desaparezca de los archivos históricos, incluso si consiguen acabar con nosotros totalmente.

Eric: ¿Y en algún momento revelaréis la clave necesaria para descodificar el material?

Julian: No. Si todo va bien, nunca la revelaremos.

Eric: Ya veo.

Julian: Porque en ocasiones este material requiere trabajo de edición.

Eric: Claro.

Julian: En nuestra opinión, el material es tan significativo que incluso su publicación tal cual tendría más beneficios que perjuicios. Aun así, con una buena edición, los daños se pueden reducir al mínimo.

Eric: Lo comprendo. Una cuestión técnica más acerca del frente: si he entendido bien, las herramientas funcionan mejor cuando un remitente anónimo envía una información a un receptor desconfiado, y luego a los anónimos [ruido] que acabas de describir. Llegará un momento en el que habrá una gran cantidad de gente utilizando esos servicios por todo tipo de razones: honradez, engaño, manipulación, lo que sea. La tecnología que usas actualmente implica básicamente el envío de lotes de FTP. En la práctica, la gente utilizará los FTP para enviaros el material[171].

Julian: No, tenemos muchas vías diferentes; lo hacemos así deliberadamente, y nunca revelamos cuál es la que más usamos porque así los recursos de investigación de nuestros oponentes tienen que dividirse entre todas las posibles vías. El material puede llegar en persona, y también por correo: el correo postal es un método bastante bueno para mandar material anónimo; basta con codificarlo con una clave secreta si se piensa que puede ser interceptado por el camino. O también puede subirse directamente a un HTTPS; no es exactamente un método directo, pero al usuario sí se lo parece. Entre bambalinas suceden todo tipo de cosas. El mayor problema con la seguridad informática no es la comunicación en sí, son sus extremos.

Eric: Cierto.

Julian: El principal problema es lidiar con los ataques contra los extremos, tanto contra aquel que intenta enviarnos información como, aún más importante, contra nuestro propio terminal que recibe dicha información[172]. Si alguien que trata de enviarnos algo está amenazado, la amenaza es a una sola persona; pero si es nuestro extremo el que está amenazado, se trata de una amenaza que potencialmente puede afectar a todas y cada una de las personas que intenten enviarnos material.

Eric: Me parece que no he formulado bien la pregunta. En tu opinión, ¿existe alguna tecnología nueva que pueda modificar materialmente el modelo simple del que dispongo sobre el fuerte incremento de…

Julian: Sí.

Eric: ¿Cuáles son entonces esas tecnologías?

Julian: La más importante es poner el nombre apropiado a las cosas. Si logramos llamar a un archivo de vídeo o de texto de tal forma que el nombre esté intrínsecamente asociado a la información contenida en el archivo y que no exista la más mínima ambigüedad, entonces esta información puede difundirse de forma que no sea preciso que las redes subyacentes sean de fiar[173]. También se puede hacer una inundación[174], o una función criptográfica segura (función hash), aunque de esta hay variantes; por ejemplo, se puede buscar una que los humanos la puedan recordar[175].

Eric: ¿Por qué no es necesario que las redes subyacentes sean de confianza?

Julian: Porque las funciones hash se pueden firmar[176].

Eric: ¿Se puede firmar el nombre además del contenido?

Julian: Basta con firmar el hash.

Eric: Ya, firmar el hash.

Julian: Si el nombre es como un hash.

Eric: En ese caso no hay ambigüedad respecto a lo que representa.

Julian: No hay lugar a error, no.

Eric: Lo que estás diciendo básicamente es que tienes un nombre fijo y verificable en lugar de uno fácilmente modificable.

Julian: Sí. Y estos tipos de mecanismos están evolucionando actualmente. Últimamente hemos estado utilizando internamente algo como esto. Yo mismo estoy escribiendo un artículo sobre ello, para intentar convertirlo en algo estándar para todo el mundo, pero se puede ver claramente que está evolucionando. Si consideramos los enlaces magnéticos… ¿los conocéis? BitTorrent ha implantado una mejora, que son los enlaces magnéticos, que realmente no son algo más que funciones hash, por lo que se trata de direccionamiento de estas funciones**[177]**. No están dirigidas a ningún servidor en concreto, sino que se trata de un gran árbol hash**[178]** muy distribuido. No sé muy bien hasta qué punto puedo ser técnico…

Eric: Por favor.

Julian: Existe un gran árbol hash distribuido por los muchos millones de ordenadores implicados, y también existen muchos puntos de entrada a este árbol hash, de forma que resulta muy difícil de censurar. Y el direccionamiento de contenidos se encuentra en el hash del propio contenido.

Eric: Entiendo. Entonces, en la práctica se utiliza el hash como una dirección, y el direccionamiento se lleva a cabo dentro del espacio de nombres que proporciona. Mientras tenga un nombre firmado, no se puede ocultar.

Julian: Bueno, depende de la información que extraigas de todo ello. Tienes un nombre de algo, un hash, pero ¿qué te dice eso? En realidad, nada, porque no es algo legible por un humano. Por tanto, necesitas otro mecanismo que saque a la luz lo que consideras importante; por ejemplo, que WikiLeaks firme algo y afirme que es…

Eric: Una información interesante.

Julian: …una información interesante, que hemos verificado como cierta**[179]**. Una vez que la información entra en el sistema, resulta muy difícil averiguar

cómo entró en él o cómo eliminarla del mismo. Y si alguien logra eliminarla, se sabe con certeza que alguien lo ha hecho, puesto que el hash ya no puede resolver nada. De forma similar, si alguien modifica la información, el hash cambia también[180].

Scott: Yo quería comentar: ¿Por qué no se limita alguien a cambiarle el nombre?

Julian: No pueden hacerlo, porque el nombre está intrínsecamente vinculado con el contenido intelectual.

Eric: Creo que la forma de explicar todo esto y resumir la idea técnica es: toma todo el contenido de un documento e imagina un número asociado a él; si el contenido desaparece, este número no muestra nada, y si el contenido cambia, el número deja de encajar. Es una forma de distinguir claramente la propiedad. ¿Falta mucho para que este tipo de sistema esté operativo?

Julian: En la parte de publicación, los enlaces magnéticos y la tecnología asociada está empezando a aparecer. Por otro lado, existen muy pocos escritos buenos sobre el Bitcoin[181]. ¿Sabes lo que es el Bitcoin?

Eric: Pues no.

Julian: Bueno, el Bitcoin es algo que se ha desarrollado a partir de los activistas *cypherpunks*, que surgieron hace un par de años[182]. Es una divisa no asociada a ningún país.

Scott: Es verdad, ayer leí algo sobre eso.

Julian: Es algo muy importante, de hecho; aún tiene algunos problemas, pero sus innovaciones superan de largo a los problemas. En este sentido, ha habido innovaciones de muchos tipos diferentes en las divisas digitales: anónimas, no rastreables, etcétera. Mucha gente ha experimentado con ellas durante los últimos veinte años. Lo cierto es que el Bitcoin tiene el equilibrio y los incentivos correctos, y esa es la razón por la que está empezando a despegar. No tiene nodos centrales; es totalmente punto a punto[183], por lo que no se necesita confiar en ningún organismo monetario central.

Si nos fijamos en las divisas tradicionales como el oro, podemos ver que tienen propiedades interesantes que las hacen valiosas como medio de pago. El oro es divisible, es fácil de cortar; de hecho, es el metal más fácil de dividir en pequeños fragmentos. Se pueden tomar esos fragmentos y fundirlos para volverlos a unir. Y se puede saber con cierta facilidad si es verdadero o falso. Esto es lo que lo convierte en un buen medio de pago. Además, conserva muy

bien su valor, ya que se puede enterrar en el suelo y sabes que no se va a descomponer, a diferencia de las manzanas o la carne.

El problema con las anteriores divisas digitales en Internet era que había que confiar en que el organismo emisor no emitiera demasiado, y este organismo tenía grandes incentivos para emitir cada vez más, puesto que la emisión es gratuita. Esto implicaba que se necesitaba algún tipo de normativa, y en este caso, ¿quién se ocupaba de velar por su cumplimiento? En definitiva, que había que tragarse todo el problema del estado, con todas las presiones políticas de la gente intentando hacerse con el control del organismo emisor, empujando hacia un lado o hacia el otro para conseguir sus propios fines.

El Bitcoin, por el contrario, tiene un algoritmo que permite que cualquiera pueda ser su propio organismo emisor. Básicamente, lo que se busca es la colisión de funciones hash[184]. Se busca una secuencia de cero bits al comienzo, y para ello hay que buscar aleatoriamente, por lo que se requiere mucho trabajo informático, trabajo que se incrementa de forma algorítmica según va pasando el tiempo. Por ello, la dificultad de producir Bitcoins se vuelve cada vez más y más y más difícil. La dificultad forma parte del sistema.

Eric: Claro, claro. Eso es interesante.

Julian: Igual que la extracción minera del oro es cada vez más difícil, y esto es lo que permite a la gente predecir que no va a haber un repentino exceso de oferta en el mercado.

Eric: Impone la escasez.

Julian: Sí, impone una escasez que se incrementará con el paso del tiempo. ¿Qué implica esto en cuanto a incentivos para entrar en el sistema Bitcoin? Pues implica que hay que entrar cuanto antes[185]. Hay que adoptarlas pronto, porque los Bitcoins que consigas hoy valdrán mucho dinero en el futuro. Una dirección Bitcoin no es más que un gran hash de una clave pública que tú mismo generas[186]. Una vez que tienes este hash, lo puedes anunciar a todo el mundo, y la gente te podrá enviar Bitcoins. Incluso hay personas que han establecido centros de cambio para convertir Bitcoins en dólares estadounidenses o en otras divisas.

La forma en que se han diseñado los Bitcoins soluciona un problema técnico muy interesante: ¿Cómo se evita el gasto múltiple con una misma unidad de divisa digital? Todo material digital puede ser clonado a coste casi cero, por

lo que si una divisa no es más que una ristra de caracteres digitales, ¿cómo impides que alguien se limite a copiarla? Quiero comprar tu paquete de pasta; aquí está mi moneda digital[187]. Pero he hecho una copia de esta moneda, y ahora quiero comprar tu docena de huevos. ¡Y ahora quiero comprar tu kilo de rábanos! Y tú piensas, «¿Cómo? ¡Esta moneda ya la tengo! ¿Qué está pasando aquí? ¡Aquí se ha cometido algún fraude!». Existe un problema de sincronización. ¿Quién tiene ahora la moneda?[188]. En una extensa red con muchas terminales es habitual que se dé el caso de que algunas partes de la red sean más rápidas que otras y que existan múltiples vías de comunicación; ¿cómo se resuelve el tema de la sincronización para determinar quién está en posesión de la moneda? En mi opinión, esta es la verdadera innovación técnica del Bitcoin: ha resuelto el problema mediante funciones hash que imponen árboles de demora y tiempos de espera. Es preciso trabajar en la CPU del ordenador para mover una cosa a la otra, por lo que la información no puede extenderse con demasiada rapidez.

Una vez que tenemos un sistema de divisas fácil de usar como hemos visto, podemos empezar a utilizarlo para otras cosas cuya abundancia se desee reducir. ¿Qué cosas deseamos que sean escasas? Los nombres. Queremos que los nombres cortos de dominio sean escasos; de otro modo, si no son escasos, si no cuesta conseguirlos, tan pronto como se consiga un buen sistema de nombramiento algún capullo va a registrar a su nombre todos los nombres cortos[189].

Eric: Es cierto. Esto es muy interesante.

Julian: Entonces, la sustitución de Bitcoins por DNS es precisamente lo que yo quería, aquello sobre lo que yo había teorizado, que en realidad no es un sistema DNS, sino más bien un servicio de archivo de tuplas texto corto-texto largo[190]. Porque esta es precisamente la abstracción. Con los nombres de dominio y todos estos problemas, lo que tienes es algo corto que deseas registrar, y que quieres asociarlo a algo largo o muy difícil de recordar.

Tomemos como ejemplo la Primera Enmienda. La frase «Primera Enmienda estadounidense» es una frase corta, pero alude a un texto algo más largo[191]. Si se toma el hash de este texto algo más largo, lo que se tiene es algo intrínsecamente asociado a él, solo que ahora es algo muy difícil de recordar. Pero este hash se puede registrar asociado a su vez a «Primera Enmienda estadounidense», lo que lleva a disponer de una estructura en la que se puede saber si algo ha sido publicado o eliminado. Un fragmento de información intelectual de la humanidad puede representar a otro de forma que la

información no pueda ser manipulada; si es censurada, la censura puede salir a la luz; y si es censurada en un sitio concreto, se puede rastrear el mundo entero en busca del hash, e independientemente de donde se encuentre, se obtiene lo que se busca.

Eric: Así es.

Julian: En teoría, esto permite a la humanidad construir un andamio intelectual en el que cada cita, cada referencia a otro contenido intelectual sea muy precisa, que pueda ser encontrada si existe en alguna parte, y que no dependa de ninguna organización particular. Como forma de publicación, esta parece ser la forma más resistente a la censura, porque no depende de ningún mecanismo de publicación. Se puede publicar a través del correo postal, del correo electrónico, de páginas web convencionales, del BitTorrent, o de la forma que sea, pero el sistema de denominaciones es siempre congruente.

La publicación también es un medio de transferencia de información. Si se desea transferir algo de forma anónima a una persona en particular, simplemente hay que codificar la información con una clave y publicarla.

Eric: Básicamente, todo el sistema depende de estructuras de claves revocables e irrevocables. ¿Te preocupa que estas estructuras se vengan abajo?

Julian: Por lo que se refiere al sistema de denominaciones, las funciones hash no dependen para nada de la estructura de claves. En términos de las propias claves, el sistema Bitcoin tiene su propia estructura de claves independiente. Esto provoca todo tipo de problemas: algún pirata informático puede robar las claves, o algo así. Son los mismos problemas que existen con el dinero en efectivo; se necesitan camiones blindados para protegerlo. Hay algunas mejoras que se pueden utilizar para intentar eliminar los incentivos de una forma u otra. Por ejemplo, se puede introducir una «subdivisa» con periodos fijos de gasto, una semana o un día, y un comerciante minorista puede aceptarla o no.

Eric: Pero el usuario medio no es consciente de que cuando RSA fue asaltada, un montón de claves muy importantes relacionadas con el comercio fueron robadas, presumiblemente por los chinos[192].

Julian: La estructura de clave pública es un problema enorme, de la misma forma que las estructuras de nombre de dominio también son problemas enormes. El sistema de clave pública que tenemos, basado en navegador para verificar qué páginas visita la gente, es horrible, verdaderamente horrible. La

cantidad de gente que ha obtenido licencia de clave nueva está fuera de control, y algunos se han arruinado y han vendido su licencia a precios baratos a compañías rusas. Podemos asumir —según me ha dicho alguien que sabe de eso, aunque aún no puedo hacerlo público porque solo dispongo de una fuente, y por lo tanto que quede entre tú y yo— que Verisign ha concedido claves al gobierno de Estados Unidos, entre ellas claves particulares firmadas[193].

Esto es un gran problema derivado de la forma en la que se verifican las cosas hoy en día. Existen algunos enfoques tradicionales alternativos; por ejemplo, PGP tiene una página de confianza[194], aunque en mi opinión estas cosas no funcionan realmente. Lo que sí creo que funciona es algo parecido a lo que hace el SSH[195], y probablemente este es el camino para avanzar. Es una clave de archivo oportunista: como parte de tu interacción, la primera vez que interactúas debes registrar tu clave, y después si dispones de varios puntos para usar esta clave y algún tipo de red inundada puedes comprobar que mucha gente ha visto esa clave muchas veces en el pasado[196].

Eric: En mi opinión, la idea del hash del nombre es algo muy interesante, porque yo no la había asociado nunca a los Bitcoins, ni tampoco ese tipo de enfoque con la escasez. Para mí es una noción totalmente nueva. ¿Habéis publicado esta idea?

Julian: El vínculo con los Bitcoins, aún no. El artículo publicado sobre el emparejamiento de algo con los Bitcoins se centraba únicamente en la cuestión de los DNS[197]. Afortunadamente, el autor de ese artículo comprendió las posibilidades: ¿por qué limitarlo a direcciones IP? Lo natural es hacerlo de forma que pueda expandirse en cualquier dirección.

La idea de que debería existir este sistema de denominaciones y de la importancia de preservar la historia, construir estos andamiajes y mapear todo… todo eso está en la página web. Creo que está en la primera parte de las entrevistas que me hizo Hans Ulrich Obrist[198].

Eric: Creo que deberíamos estudiar esto bastante más para entenderlo mejor. Puede que tengamos algunas preguntas más al respecto. El otro comentario que me gustaría hacer es que, asumiendo que lo que describes vaya a ocurrir realmente, lo que en mi opinión es muy probable, dado que la estructura de incentivos es…

Julian: Oh, hace varios años que tengo estas ideas, pero ahora comienzo a ver como otras personas también empiezan a…

Eric: Bueno, hay suficientes personas interesadas en resolver el mismo problema que tú estás tratando de resolver. En Internet se ve mucho [*inaudible*]. La cuestión que se me pasa por la mente ahora mismo es, ¿cómo lo atacaría yo? ¿Cómo atacaría tu idea? Y sigo pensando que yo me centraría en la firma y la infraestructura de claves. Por eso, si puedo romper las claves…

Julian: La idea tiene diferentes aspectos. Es bastante interesante para cuando algo pasa de estar sin publicar a estar publicado. Si publicas alguna información y la etiquetas bien mediante un hash, ese hash es importante; tiene que difundirse de otra manera, por ejemplo con la firma de WikiLeaks. Pero existen muchas formas de difusión: la gente puede intercambiar ese hash por correo electrónico, se puede comunicar por teléfono, etcétera.

Eric: Lo que estás diciendo es que todos estos sistemas no tienen un único punto de ataque, ¿no? Yo puedo entrar en tu HTTPS, pero tú aún puedes usar el servicio postal para enviar lo que sea, por ejemplo.

Julian: Exactamente, y sabrías que lo que obtienes es lo correcto gracias a la denominación. Es muy muy preciso.

COMUNICÁNDOSE EN UN MOMENTO REVOLUCIONARIO

Eric: Al principio estuvimos hablando sobre mi idea de que los teléfonos móviles tienen el poder de cambiar la sociedad. Para los que no estaban, un resumen aproximado de tu respuesta sería que la gente sigue siendo más o menos la misma, que algo grande debe cambiar su comportamiento, y que puede que esto sea uno de esos algos. Dijiste que estabas muy interesado en la creación de criptografía para utilizar entre teléfonos. ¿Podrías hablar un poco sobre la arquitectura aproximada en la que existiría una red abierta con códigos persona a persona? ¿Qué implicaría ello en el plano técnico, cómo funcionaría, por qué sería importante y todo eso? Me da la impresión de que la gente no entiende nada de lo relacionado con este ámbito.

Julian: Cuando estábamos ocupados con el caso de Egipto, vimos que el gobierno de Mubarak cortó las conexiones a Internet, pero hubo un proveedor que mantuvo su conexión, pues bastantes de nosotros pusimos todos nuestros

esfuerzos en que así fuera, proveedor que suponía aproximadamente un 6 % del mercado[199]. El gobierno también interrumpió el sistema de telefonía móvil. ¿Cómo es que se puede hacer esto? Las personas con teléfono móvil tienen un dispositivo que puede comunicarse mediante ondas de radio. En una ciudad suele haber una alta densidad de teléfonos móviles, por lo que siempre existe un camino entre una persona y otra, esto es, siempre hay un camino continuo de teléfonos móviles, en el que cada uno de ellos puede, en teoría, escuchar la radio de los demás.

Eric: ¿Entonces se podría crear una red entre usuarios?[200]

Julian: En teoría sí, se podría crear una red entre usuarios. Por la forma en la que se fabrican la mayoría de los móviles GSM y de otro tipo, la frecuencia en la que reciben no es la misma que aquella en la que luego transmiten, y ello significa que no pueden formar redes entre usuarios iguales[201], sino que tienen que pasar por estaciones de emisión[202]. Pero últimamente estamos viendo que los teléfonos móviles se están haciendo cada vez más flexibles en términos de programación de base; tienen que serlo, porque se venden en diferentes mercados, con diferentes frecuencias y diferentes formas de transmisión[203]. Incluso para los móviles que no son lo suficientemente flexibles, actualmente se está desarrollando mucho la tecnología WiMAX, que les proporcionará un radio más amplio para la comunicación bilateral[204]. Además, cada vez se está haciendo más barato crear tu propia estación emisora, y hasta existen *softwares* que la pueden gestionar por ti[205]; gracias a ello, se pueden crear redes propias mediante teléfonos móviles convencionales. De hecho, esto es lo que se suele hacer para espiar de forma barata: basta con instalar una estación emisora falsa en una furgoneta, que se puede adquirir con el equipo completo, para interceptar llamadas telefónicas.

Durante los periodos revolucionarios, las personas muy implicadas necesitan ser capaces de transmitir rápidamente información sobre su entorno para adaptarse dinámicamente a ella y planificar la siguiente estrategia. Si el gobierno desconecta el sistema de telefonía móvil, y únicamente los servicios de seguridad son capaces de comunicarse, estos servicios cuentan con una enorme ventaja[206]. Si tienes un sistema en el que los individuos son capaces de comunicarse de forma segura y eficaz hagan lo que hagan los servicios de seguridad, entonces estos últimos tendrán que ceder terreno. No significa que el gobierno vaya a ser derrocado necesariamente, sino que tendrán que hacer más concesiones.

Eric: Tienen sus propias redes. Entonces, tu argumento es que incluso los teléfonos móviles ya existentes podrían ser modificados para disponer supuestamente de túneles codificados para enviar voz y datos directamente entre usuarios[207].

Julian: La voz es un poco más difícil. Yo mismo he diseñado un prototipo, pero solo funciona para grupos de tamaño medio. Es una red inundada entre usuarios codificada con un UDP[208], que te permite una gran capacidad de transmisión de información, puesto que se pueden enviar datos aleatorios a páginas web aleatorias[209].

Eric: Oh, eso es genial. Así no te pueden bloquear, ¿no?

Julian: Eso es.

Eric: Porque el UDP es un solo paquete, ¿verdad?

Julian: Exacto. Y lo envías a páginas aleatorias, y estas páginas no responden, como suele ser habitual. De esta forma se pueden atravesar los cortafuegos[210]. Esto implica que la gente puede utilizar esto desde su casa; no necesita tener un servidor[211]. Y el ancho de banda es muy pequeño, por lo que se pueden utilizar teléfonos móviles también[212].

La aplicación asesina no está relacionada con la voz[213], sino con los grupos de chat. Lo que necesitan los movimientos revolucionarios son pequeños grupos de entre treinta y cien usuarios, seguros y eficaces. El sistema que yo diseñé era un protocolo independiente[214]. Tienes tu resumen de la información —UDP o lo que sea— y en teoría lo puedes enviar por SMS, por TCP o de la forma que quieras[215]. Puedes usar un teléfono móvil, un ordenador portátil, etcétera. Lo puedes poner en red, de forma que incluso si el país entero está desconectado, basta una simple conexión vía satélite y tus redes internas pueden conectarse al resto del mundo.

Eric: Claro, claro.

Julian: Si la red es pequeña se puede usar la inundación. Una red inundada recorre todos los caminos posibles, por lo que por fuerza debe tomar también el más rápido. Este tipo de red siempre encuentra un camino aunque no suele alcanzar grandes proporciones. Sin embargo, si dispones de un buen sistema de rutas electrónicas, lo único que necesitas es un enlace para salir. Y en Egipto teníamos a gente que había logrado piratear la página web de Toyota en El Cairo, apropiándose de su conexión vía satélite y utilizándola para

conectarse a este ISP que tenía el 6 % del mercado. Este tipo de cosas ocurrían constantemente. En el país había una guerra de piratas informáticos que intentaban mantener activo este ISP independiente, lo que no debería haber sido tan difícil: todo cuanto se necesitaba era una conexión, con ella la información más importante podría salir sin problemas.

Mira lo importantes que son Twitter y el SMS. Los seres humanos son bastante buenos a la hora de codificar el evento más importante que esté ocurriendo y reducirlo a una pequeña cantidad de datos. No hay tantos seres humanos, sencillamente no los hay.

Eric: No es un problema de ancho de banda[216].

Julian: No, no es un problema de ancho de banda. Todo lo que se necesita es una simple tubería y puedes conectar un país entero que está en plena revolución al resto del mundo[217]. Y lo que es más importante, puedes conectar diferentes puntos y ciudades dentro de ese país. Francamente, en realidad no es algo tan difícil.

Eric: Scott, ¿quieres…?

Scott: ¡Es difícil parar! ¡Esto es tan interesante!

Eric: Lo cierto es que tengo como cinco horas más de preguntas técnicas.

Scott: ¡Lo sé! Es que es primero una cosa y luego muchas otras.

Eric: ¿Cómo proyectarías esto, cómo proyectarías aquello…?[218]

LA CENSURA SIEMPRE ES MOTIVO DE CELEBRACIÓN

Scott: Estaba pensando en el lado humano de todo esto. Antes has hablado de tu experiencia en el mundo… He dormido solo tres horas, así que perdona si no recuerdo exactamente lo que has dicho, pero hablabas de la combinación de técnicos con personas altruistas, y lo que viene a ser una especie de subcultura en la que has estado implicado desde hace unos quince años. Ahora sabes cómo funciona esta subcultura, si necesita seguir como está o crecer para hacer el trabajo que has descrito. Por tanto, puesto que a nuestro libro aún le quedan diez años…

Julian: Se ha ampliado radicalmente.

Scott: ¿Cuáles son los patrones de comportamiento de la parte humana, más que de la parte técnica?

Julian: Esa es la parte más optimista de todo lo que está pasando: la juventud educada con Internet, es cada vez más radical; la gente está recibiendo sus valores de Internet y, al estar de acuerdo con ellos, los reproduce. Actualmente, esta repetición es tan fuerte que ahoga completamente las declaraciones precedentes.

La gente con la que he tratado desde los movimientos radicales de los años 60 que ayudaron a liberar Grecia y a luchar contra Salazar en Portugal dicen que lo que está ocurriendo en este preciso momento es muy parecido a lo que ocurrió en aquel periodo de movimientos de liberación[219].

Scott: ¿Ves una evolución diferente a la de los sesenta?

Julian: En los sesenta yo aún no había nacido, pero hasta donde yo sé, en Occidente —porque hay algunas regiones del mundo que no conozco— sus apreciaciones son correctas. La educación política de técnicos apolíticos es extraordinaria. Los jóvenes están pasando de ser apolíticos a interesarte por la política. Es una transición muy, muy interesante de ver.

Scott: Este es nuestro mundo. ¿Por qué piensas que ha ocurrido esto?

Julian: Comunicaciones rápidas, masa crítica de gente joven, nueva generación y algunos eventos catalizadores. El ataque a WikiLeaks fue uno de estos eventos, y nuestro éxito al defendernos de este ataque fue otro de ellos. ¿Recordáis el caso PGP, el gran jurado contra Zimmermann?[220]

Eric: Se lo pasó muy bien con todo eso.

Julian: Una vez escribí la mitad de un libro sobre el tema. Nunca lo publicaron, porque a mi coautora le dio por tener hijos.

[En este momento, Lisa derrama agua sobre su ordenador portátil, en el que está tomando notas. Julian toma instantáneamente el ordenador y le da la vuelta para que caiga el agua]

Lisa: ¡Oh no! ¡Ja ja ja ja!

Eric: ¡Ja ja ja!

Jared: ¿Por qué tengo la impresión de que esto ya ha pasado antes?

Lisa: Ha sido muy divertido.

Scott: ¡Adiós al archivo histórico!

Julian: Como dije antes: ¡Copias múltiples!

[Risas]

Eric: ¿Por qué no grabas lo que estás haciendo?

Scott: Vamos a hablar del árbol de nombres antes de que todo se acabe de estropear.

Lisa: ¿Habéis visto que rápido ha sido? Fue instintivo.

Jared: Sí, creo que casi agarró el ordenador antes de que el agua lo tocase.

Eric: Los ordenadores son importantes en nuestro trabajo.

[Risas]

Lisa: Has sido muy amable, gracias. Podéis seguir.

Scott: Pero los jóvenes no son buenos por naturaleza. Y lo digo como padre y con pesar.

[Risas]

Julian: Oh no, yo pienso que realmente… Bueno, he leído *El señor de las moscas* y he ido como a treinta colegios diferentes, así que he visto muchas situaciones similares a la del libro[221]. Pero no, pienso que los instintos de los seres humanos sean realmente mucho mejores que las sociedades que tenemos.

Eric: Que los gobiernos, más bien.

Julian: Yo no diría gobiernos. Más bien toda la estructura de la sociedad, y la estructura económica. La gente aprende que los actos altruistas no se ven recompensados, y también ve que algunas personas que actúan de forma poco altruista acaban pudiendo comprar Porsches, lo que les impulsa en esta dirección. Esto se me ocurrió hace un tiempo, cuando vi un vídeo fantástico elaborado en Stanford en 1971, sobre la síntesis nuclear del ADN[222]. ¿Lo habéis visto?

Scott: No.

Julian: Está en YouTube. Es algo genial. Explica la síntesis nuclear mediante una coreografía. Salen como 130 estudiantes de Stanford en mitad de un campo de deportes fingiendo ser ADN; un grupo representando la subunidad ribosómica, todos ellos llevando el atuendo *hippy* típico de esos años, aunque en realidad eran alumnos brillantes. Es un vídeo realmente educativo; no es solo que fuese algo llamativo e inusual, que también, sino que para la época era extremadamente instructivo, pues antes de la llegada de la animación por ordenador era la mejor representación que se podía tener de cómo funciona una unidad ribosómica. ¿Os imagináis a Stanford haciendo esto hoy en día? Imposible. Actualmente es una institución demasiado conservadora para llevar a cabo algo así, a pesar de que en su momento fue realmente efectivo. Apuesto lo que sea a que todos los que participaron en esa coreografía aún recuerdan exactamente cómo tiene lugar la síntesis nuclear, porque todos tuvieron que aprenderse su parte de memoria. Y yo recuerdo perfectamente haberlo visto.

El periodo con el salario medio más alto en Estados Unidos fue en torno a 1977, ¿no?**[223]** Pero entonces ocurrieron ciertas cosas. Aquellas personas que eran altruistas y no se preocupaban mucho por las finanzas y el control fiscal sobre las personas simplemente perdieron poder adquisitivo respecto de aquellas otras que sí se preocupaban de esas dos cosas y que empezaron a escalar posiciones dentro del sistema. Se desincentivaron ciertos comportamientos y se potenciaron otros, en mi opinión como resultado de la tecnología que permitía el control fiscal: transferencias bancarias rápidas, capacidad de controlar a mucha gente con el IRS**[224]**… todo ello encerró a la gente en una estructura controladora muy rígida.

En Estados Unidos se pueden producir muchos «cambios» políticos, pero estos cambios políticos ¿realmente cambiarán muchos las cosas? ¿Cambiarán el saldo de la cuenta corriente de la gente? ¿Cambiarán los contratos? ¿Invalidarán los contratos ya existentes? ¿Y los contratos sobre los contratos? ¿Y los contratos sobre los contratos sobre los contratos? En realidad no. Por ello, en mi opinión la libertad de expresión en muchos países occidentales no es el resultado de unas condiciones de libertad, sino más bien es el resultado de que con un sistema de control tan intenso en realidad da igual lo que digas. A la élite dominante ya no le asusta lo que piense la gente, porque un cambio de visión política no va a cambiar el hecho de que sean propietarios o no de una compañía o de un terreno. Pero China sigue siendo una sociedad con predominio de la política, pese a estar transformándose rápidamente en una

sociedad controlada. Y otras sociedades, como Egipto, aún siguen estando fuertemente politizadas. Sus gobernantes necesitan realmente preocuparse por lo que piensa la gente, y por ello dedican mucho esfuerzo al control de la libertad de expresión.

Sin embargo, pienso que la gente joven sí tiene valores innatos bastante positivos. Por supuesto, hay de todo, pero en la mayoría de los casos sus valores son buenos; desean demostrarlo al resto de la gente, y cuando más se ve esto es cuando ingresan en la universidad. Después hay muchos que se endurecen debido a que ciertas cosas tienen recompensa y otras no la tienen.

Scott: Déjame aclarar un poco esto. Parece que tienes una visión del mundo según la cual hay algunas sociedades en las que el impacto de la tecnología es relativamente pequeño, otras en las que el impacto político de esta tecnología podría ser bastante grande, y otras en las que sería algo intermedio. Por lo que dices, parece que sitúas a China en este último grupo. Dado que nuestro libro tratará sobre la transformación tecnológica y social de aquí a diez años, con el esquema que has descrito ¿cómo verías tu el mundo?

Julian: No estoy seguro sobre el impacto en China. Sigue siendo una sociedad con predominio de la política, por lo que el impacto podría ser muy grande. Yo suelo decir que la censura es motivo de celebración: siempre es una oportunidad porque revela miedo a la reforma; significa que el poder tiene una posición tan débil que tiene que cuidarse de lo que piensa la gente.

Jared: Eso es un razonamiento interesante.

Eric: Es un razonamiento muy interesante.

Scott: Es como descubrir los documentos confidenciales simplemente observando cómo se cazan.

Julian: Exacto. Así, cuando los chinos emplean toda esa energía en censurar de formas cada vez más novedosas, ¿diremos que es una absoluta pérdida de tiempo y energía, o que tienen mucha experiencia a la hora de gestionar el país y comprenden que lo que la gente piensa es importante? Yo creo que es mucho más razonable interpretarlo como que los controladores de la censura en China son muy conscientes de que su posición de poder es débil, y necesitan tener mucho cuidado con lo que piensa la gente. Por tanto, tienen que censurar.

Scott: Entonces el estado es racional, al menos dentro de su represión.

Julian: A mí siempre me preocupa que se hable del estado porque en realidad siempre son individuos actuando en su propio interés. Este grupo o aquel grupo.

Scott: Así es.

Julian: Consideremos por ejemplo las personas que trabajan como censores en el Ministerio de Seguridad Pública en China. ¿Por qué censuran, y qué censuran primero? Te voy a decir lo que censuran primero: ¡aquellas páginas que pueden ver los empleados del Buró político del gobierno! Eso es siempre lo primero. En realidad no se preocupan mucho por las redes oscuras[225].

Jared: Perdona, ¿por qué has dicho eso?

Julian: No les preocupan las redes oscuras porque sus jefes no pueden ver lo que hay en ellas, y por tanto no se les puede acusar de no haberlo censurado.

Aquí en Reino Unido tuvimos un caso fantástico en el que publicamos un montón de documentos clasificados del ejército británico. Poco después hicimos un FOI preventivo, algo que hacemos de vez en cuando, cuando podemos, con diversos gobiernos[226]. Lo hicimos sobre el Ministerio de Defensa de Reino Unido para ver si estaban llevando a cabo algún tipo de investigación y así proteger mejor nuestras fuentes. Al principio no nos dieron los documentos, pero recurrimos y conseguimos parte de ellos. Alguien en el Ministerio había visto que en nuestra página había una gran cantidad de documentos militares británicos sobre su programa de vigilancia, así como un documento de dos mil páginas redactado por ellos, en el que se explicaba la forma de evitar filtraciones y se afirmaba que la principal amenaza del ejército británico eran los periodistas de investigación[227]. Esto había llegado a oídos de alguien de contraespionaje y esta persona había dicho: «¡Oh, Dios mío, hay cientos de páginas sobre todo tipo de países, y no parece tener fin! ¡¡Es infinito!! ¡¡¡¡¡Infinito!!!!!» Cinco signos de admiración. Eso fue la fase de descubrimiento, pero ahora estamos en la fase «qué vamos a hacer al respecto». Como BT tiene los contratos del Ministerio de Defensa (MdD)[228], el Ministerio le dijo a BT que nos censurase, para que nadie del propio Ministerio pudiese leer lo que salía en WikiLeaks. ¡Problema resuelto!

Eric: Interesante.

Julian: Sus generales y sus jefes ya no podían ver que teníamos información sobre el MdD en WikiLeaks; se acabaron las protestas y su problema quedaba solucionado. El conocimiento de este hecho puede ser muy ventajoso en

algunos de estos sistemas: si eres consciente de que en las estructuras burocráticas siempre ocurre este tipo de cosas, sabes que las redes oscuras van a estar bastante tranquilas, al menos hasta que sean tan grandes que dejen de ser redes oscuras.

Scott: Eso es muy, muy interesante. Antes has mencionado el periodismo de investigación. Tú que has tenido mucha experiencia en muchos ámbitos del periodismo, ¿qué opinas de la clase de libertad de información que describías antes? ¿Encaja en los procesos periodísticos, o los está reemplazando?

Julian: No, se trata más bien de cómo encajan estos procesos periodísticos en algo que es mucho mayor, y esto es que como seres humanos dirigimos y creamos nuestra historia intelectual como civilización. Y es esta historia intelectual la que podemos utilizar para hacer cosas, y para evitar volver a hacer cosas estúpidas, pues alguien ya las hizo primero y escribieron su experiencia, por lo que ya no necesitamos volver a hacerlas. Hay varios procesos diferentes que están creando ese archivo, y otros procesos en los que determinada gente está intentando destruir bits de ese archivo, y otros más que están intentando evitar que la gente añada cosas a ese archivo. Todos vivimos de y en ese archivo intelectual. Lo que queremos hacer es meternos lo más posible en ese archivo, hacer todo lo posible para evitar ser eliminados de ese archivo, y lograr que el archivo sea lo más visible posible.

Eric: Pero una consecuencia de esta forma de ver las cosas es que a algunos de los participantes en el proceso puede beneficiarles la creación de grandes cantidades de desinformación.

Julian: Sí. Eso es otro tipo de censura que me viene a la mente a menudo pero de la que hablo pocas veces, que es la censura mediante la complejidad.

Eric: Es verdad. Demasiada complejidad.

Julian: Y eso es básicamente lo que ocurre con los paraísos fiscales: la censura mediante la complejidad. ¿Censura de qué? Censura de la indignación política. Si se alcanza la suficiente indignación política se consiguen reformas en la ley, y con reformas en la ley ya no se puede hacer esto. ¿Por qué son entonces tan complejos todos los meticulosos entramados de ingeniería fiscal? Puede que sean perfectamente legales, pero ¿por qué son tan jodidamente complejos? Pues porque los que no lo eran se comprendían fácilmente, y aquellos que se comprendían eran regulados, por lo que solo quedan las cosas increíblemente complejas.

Scott: A mayor ruido, menor señal.

Julian: Sí, exactamente.

Eric: Pero en el futuro, ¿cómo lidiará la gente con el hecho de que exista un gran incentivo para publicar información engañosa, falsa o manipuladora? Además, no se puede saber quién ha sido el editor malo y quién el bueno, porque el sistema es anónimo.

Julian: Primero debemos entender que la situación actual es muy mala. Un periodista de *The Nation*, Greg Mitchell, que también ha escrito artículos sobre nosotros, escribió un libro sobre los medios de comunicación importantes llamado *So Wrong for So Long*[229] («Tan injusto durante tanto tiempo»). El título lo dice todo. Sí, tenemos algunos momentos heroicos, como el Watergate y cosas así, pero en realidad, seamos sinceros, la prensa nunca ha sido muy buena; al contrario, siempre ha sido muy mala. Los buenos periodistas son la excepción que confirma la regla. Cuando estás implicado en algo, como yo lo estoy con WikiLeaks, y conoces cada faceta de ese algo, si lees lo que se publica sobre ello te encuentras con una mentira detrás de otra, y sabes que los periodistas saben que son mentiras, que no se trata de simples errores. Luego la gente repite esas mentiras, y la cosa empeora. El estado de los grandes medios de comunicación es tan horrible que sinceramente no creo que pueda reformarse; creo que no queda otro remedio que eliminarlos por completo y sustituirlos por otros mejores.

Scott: ¡Algo que parece que está ocurriendo ya!

Julian: Sí, y yo mismo he promocionado esta idea del periodismo científico: que la información debe citarse con precisión e indicando la fuente original, y que se ponga a disposición del público la mayor cantidad de información posible para que pueda leerla, igual que se hace en el sector científico, para comprobar si de tales datos se deriva efectivamente tal conclusión[230]; de otro modo, es probable que el periodista simplemente se lo haya inventado todo. De hecho, esto pasa todo el tiempo: la gente sencillamente se lo inventa, a veces hasta tal punto que nos llevan a la guerra por ello. La mayoría de las guerras del siglo XX comenzaron como resultado de mentiras amplificadas y difundidas por la prensa. Muchos dirán: «Eso es algo horrible; es terrible que todas estas guerras comenzasen con mentiras». Y yo digo que no, que se trata de una extraordinaria oportunidad, porque ello significa que a la inmensa mayoría de la gente no le gustan las guerras y tiene que ser engañada para entrar en ellas, lo que a su vez implica que se puede llegar a la paz a través de la verdad. Esto es motivo de gran esperanza.

Pero la cuestión de cómo distinguir a los editores honestos de los deshonestos tiene que ver con la reputación. Lo que a mí me gustaría es ver que se introduce en el periodismo ese aspecto tan relacionado con la reputación de la ciencia que es la pregunta: «¿Dónde están los datos?». Si no se aportan datos, ¿por qué demonios debería tomarme esto en serio? Ahora que se puede publicar en Internet, ahora que hay espacio de sobra para incluir datos, deberían incluirse siempre. Los periódicos en papel no tienen sitio en sus páginas para incluir la fuente, pero ahora que sí lo tienen en su versión digital, se debería obligar a su inclusión. La gente puede saltarse esta norma, pero si lo hacen y tampoco se molestan en aportar datos, ¿por qué deberíamos prestar la más mínima atención a lo que escriben? No están tratando al lector con el debido respeto.

Supongo que en realidad el tema de la reputación es importante. ¿Cómo se adquiere una reputación? En parte mediante una serie de citas. Ocurre algo, alguien dice algo sobre ello, alguien más dice algo sobre ello, y así sucesivamente. Es una serie de citas que fluye de una persona a otra, y para que adquieran fuerza se necesita un sistema de nombramiento sólido, en el que la base no sea una página web que desaparezca mañana, o que modifique la información porque a una compañía no le guste, o que le lluevan las demandas. En mi opinión, eso ayudaría a construir una reputación.

La complejidad es más difícil de tratar, y creo que ello supone un gran problema. Cuando las cosas salen a la luz tienden a volverse más complejas, porque la gente comienza a ocultar lo que está haciendo —su mal comportamiento— mediante complejidad. Un ejemplo es el ambiguo lenguaje burocrático: cuando la información se burocratiza, todo se vuelve poco claro; es el coste de la apertura. En los paraísos fiscales se pueden ver niveles increíbles de complejidad en todo lo que allí ocurre, por lo que todo se vuelve impenetrable. Por supuesto, la criptografía es un sistema intelectual que se ha especializado en hacer que la información sea lo más compleja posible, que sea difícil de atacar. Por otro lado, los sistemas complejos también son difíciles de utilizar. Las burocracias y los sistemas de comunicación interna que están plagados de palabras engañosas y de gente cubriéndose el culo son sistemas ineficientes, al igual que esos complejos acuerdos de ingeniería societaria en los paraísos fiscales. Puede que vayas un paso por delante cuando el régimen fiscal es elevado, pero si es de solo el 3 %, no hay forma de librarse: la complejidad te va a ahogar.

Scott: Bueno, Julian, si no fuesen ineficientes, todo el mundo tendría su dinero en paraísos fiscales.

Julian: Sí, eso es verdad.

Scott: Era una broma, pero probablemente es cierto.

Julian: Probablemente no, es cierto. Hay un combate desencadenado entre todas estas cosas. Yo no veo diferencia alguna entre los gobiernos y las grandes y pequeñas corporaciones. Es todo un continuo: sistemas que intentan conseguir todo el poder que les sea posible. Un general intenta que su sección del ejército tenga el mayor poder posible, y todos los demás igual: hacen publicidad, producen algo que sostienen que es un producto, la gente lo compra o no lo compra, crean complejidad para ocultar los fallos de su producto, y dan vueltas y más vueltas. En este sentido, como digo, no veo diferencias entre los dirigentes de los gobiernos y los de otros organismos entidades no gubernamentales. Quizá existe una diferencia teórica relacionada con la capacidad para desplegar fuerzas coercitivas, pero incluso en este caso está claro que las corporaciones bien conectadas pueden interferir en los gobiernos o en los tribunales de justicia, y por tanto son muy capaces de ejercer la fuerza empleando a la policía para recaudar deudas o para echar a empleados de la oficina.

EL SECRETISMO ES CRIMINÓGENO

Scott: Déjame preguntarte más o menos lo mismo pero al revés: ¿de qué formas pueden las fuentes de información, en tanto que individuos, ser protegidas o no? En otras palabras, ¿cómo puede ser anónima su información, de forma que no paguen el precio de ponerla en circulación? Tal vez sirva un ejemplo de Corea del Norte o Irán y otro ejemplo de Estados Unidos, para ver las diferencias de esos dos escenarios.

Julian: Existen muchas vías para que la gente pueda transmitir información de forma anónima. Una de las principales dificultades de las fuentes es su proximidad al material. Si están muy próximas a una determinada información y hay un número limitado de personas que tienen acceso a ella, lo cierto es que da igual qué mecanismo técnico apliquen, pues les resultará muy difícil eludir el escrutinio, independientemente del país o del régimen

político en el que estén. Pero, por definición, la injusticia sistemática afecta a mucha gente, y, aunque no se pueda extraer cierta documentación de lo más profundo del sanctasanctórum de un consejo de ministros, si las decisiones que toman producen consecuencias injustas que afectan a mucha gente, entonces muchas personas del entorno de los que deciden tienen que ver al menos la sombra de los planes secretos de alto nivel, como por ejemplo las instrucciones para su implementación que reciben los niveles inferiores; puede que el plan completo sea invisible para los curritos, pero sus componentes tienen que verse.

Esto me llamó la atención cuando llegaron a nuestras manos los dos principales manuales operativos de la base de Guantánamo. El manual de 2003 fue el primero que obtuvimos, redactado por el general de brigada Geoffrey Miller, quien posteriormente se trasladaría a Abu Ghraib para «convertirla en otro Guantánamo», en palabras de Donald Rumsfeld[231]. Este manual incluía todo tipo de abusos[232]. Una de las cosas que más me sorprendió fue la instrucción explícita de falsificar los informes enviados a la Cruz Roja. ¿Cuánta gente había leído este manual? Todos los capitanes de prisiones de la bahía de Guantánamo lo habían hecho. ¿Por qué se arriesgaría nadie a difundir esta información entre los trabajadores de a pie? Ni siquiera era documentación clasificada, estaba simplemente clasificada como «Exclusivamente para uso de oficiales». ¿Por qué? Pues porque es más caro conseguir personas con acceso autorizado a información clasificada; por ejemplo, es más barato encontrar contratistas sin esta autorización. No se puede cuchichear en la mina de carbón[233]. No se puede pretender que el presidente susurre en la mina de carbón, porque la veta es demasiado grande, y tampoco se puede pretender que el presidente cuchichee con los intermediarios, porque en este caso se acaba jugando a los susurros chinos[VI], y las instrucciones no se cumplen al pie de la letra. Si no se pone la información en un soporte físico, sea este en papel o electrónico, las instrucciones se diluyen, y por ello todas las organizaciones, grandes o pequeñas, tienen registradas cuidadosamente las instrucciones procedentes de sus líderes. Además, por definición, si se intenta que mucha gente haga algo, hay que dar instrucciones escritas lo que quiere decir que siempre habrá un rastro en papel. Las decisiones de los pequeños grupos que no bajan hasta la mina son una excepción, pero si estas decisiones de los grupos pequeños no bajan para instruir a mucha gente, ¿realmente son importantes a nuestros efectos?

Scott: Ciertamente, serían poco efectivas.

Eric: Cuando estuvimos en Berlín, visitamos el lugar donde firmaron la orden final, ¿cómo se llamaba?

Lisa: La Solución Final. Wannsee[234].

Eric: Eso es, Wannsee, y estamos hablando de alemanes, que normalmente documentan absolutamente todo.

Lisa: Es fascinante.

Eric: Y esto es exactamente lo que estás diciendo. Para matar a seis millones de judíos, realmente hay que dejar instrucciones por escrito.

Julian: Es un gran proceso logístico.

Eric: Justamente, y había muchísimas cosas que comunicar: cuáles eran los procedimientos, estas son las fotos y las firmas de las personas, etcétera, etcétera.

Lisa: El acta de la reunión.

Eric: Fue algo realmente espeluznante. La banalidad del mal[235].

Lisa: Y que lo digas.

Julian: Sí, pero este es uno de los primeros debates internos que yo tuve con otras personas en 2006. Ellos me decían: «Bueno, vale, puedes sacar a la luz los trapos sucios de alguna organización y mostrar que ha estado abusando de algo de alguna forma, pero lo que hará entonces es eliminar todas las instrucciones escritas y hacerlas orales». Y yo dije: «No, eso no va a ocurrir, porque si hacen eso, si eliminan toda las instrucciones escritas, si balcanizan la información interna de forma que no pueda filtrarse, incurrirían en un coste tremendo por ineficiencias organizativas. Y si aun así se empeñan en hacerlo, el resultado sería que esta organización abusiva simplemente se volvería menos poderosa en su lucha por el equilibrio económico y político respecto de otras organizaciones».

Eric: Este argumento es el inverso del que utilizaste para el empoderamiento de los disidentes en Egipto. Ellos necesitaban los SMS para comunicarse, y en este caso se trata de evitar la incapacidad de coordinarse a este nivel. Literalmente, lo contrario del primer argumento. En tu opinión, si se eliminan esas herramientas…

Julian: Sí, bueno, yo diría que son ellos mismos los que las eliminan. Existen toda clase de razones por las que las organizaciones con poco poder practican el secretismo, que en mi opinión es algo legítimo; lo necesitan precisamente porque no tienen poder. Pero ¿por qué lo hacen las organizaciones poderosas? Bueno, normalmente se debe a que si se publican los planes que tienen, la gente se opondría a ellos. Los planes que encuentran una fuerte oposición antes de su implementación a menudo no llegan a implementarse, por lo que suelen esperar el máximo tiempo posible antes de publicarlos. La implementación de los planes conlleva forzosamente su publicación, pero para entonces es demasiado tarde para alterar el curso de la acción de forma efectiva.

Por otra parte, una organización cuyos planes de acción no encuentran la oposición del público no tiene que afrontar esa dificultad, y por tanto no se ve impelida a eliminar las instrucciones escritas. Esta será una organización eficiente, a diferencia de la otra, que será ineficiente, y en la batalla económica y política, la organización eficiente crecerá y la ineficiente decrecerá.

Eric: ¿Consideras que esta es la principal justificación de lo que estáis haciendo?

Julian: En realidad, hay dos justificaciones fundamentales. En primer lugar, la civilización humana, o al menos su parte buena, está basada en el conocimiento de su historia, y si la humanidad desea ser lo más avanzada posible este conocimiento debería ser lo más amplio posible. Y en segundo lugar, en la práctica publicar información es positivo para aquellos que están involucrados en actos que el público apoya y negativo para los que están involucrados en actos que el público no apoya.

Eric: Entonces es una forma de control.

Julian: Puede reconducir un acto de injusticia cuando este sale a la luz, lo cual está bien. Pero el efecto a largo plazo es que reduce los incentivos de las organizaciones para crear planes injustos o implicarse en actos injustos.

Eric: Una pregunta más relacionada con esto. En diez años, ¿qué aspecto tendrá este mundo? Es decir, si extrapolas el argumento.

Julian: Bueno, ahora mismo estamos en una encrucijada, ¿no? Podría tomar cualquier dirección.

Scott: ¿Cuál sería el escenario optimista y cuál el pesimista?

Julian: ¿Recordáis el caso del PGP de Philip Zimmermann?

Eric: Sí.

Julian: Aquello fue solo una investigación de un gran jurado. Fue algo moderadamente serio, pero no fue condenado por ello. En aquel momento nadie fue siquiera imputado; era solo una investigación. Pero lo que hizo fue cambiar el comportamiento de decenas de miles de personas implicadas en ello a la hora de usar o no criptografía en los programas[236]. Debido a la señal negativa enviada por esa investigación del gran jurado, surgieron todo tipo de distorsionadas asignaciones de *copyright* y acuerdos de estructuración entre *softwares* corporativos. Las señales sobre qué comportamiento es aceptable, con qué comportamiento puedes salirte con la tuya, qué comportamiento es beneficioso para los individuos implicados en él y qué comportamiento no lo es, modifican el comportamiento de mucha gente.

Ahora mismo estamos en una encrucijada en la que las organizaciones que están luchando contra aquellas personas que desean poder publicar libremente y revelar información importante al público… Ahora no recuerdo el comienzo de la frase.

Jared: Decías que ahora mismo estamos en una encrucijada en la que las organizaciones que están luchando contra aquellas personas que desean poder publicar libremente y revelar información importante al público.

Julian: Vaya lapsus, ¿no? Eso es, ja ja. Estamos en una encrucijada en la que esas organizaciones que están luchando contra aquellas personas que desean poder publicar libremente y revelar información importante al público podrían emitir, si tienen éxito, una señal que desaliente a casi todo el mundo a participar en esas actividades. O podríamos ser nosotros y la gente que comparte nuestros valores los que tengamos éxito y consigamos que este comportamiento se convierta en la nueva norma.

Scott: Me puedo imaginar fácilmente cuáles serían las condiciones necesarias para lo primero, pero ¿cuáles serían las condiciones necesarias para que ocurra lo segundo?

Julian: ¡Que todo el mundo dé dinero a WikiLeaks!

[Risas]

Scott: ¿Aceptáis Bitcoins?

Julian: ¡Por supuesto! Sería interesante saber si cuando la gente lea esto y actúe en consecuencia, su acción será suficiente para cambiar el resultado. Esta es la razón por la que estamos en un periodo muy interesante. Creo que estamos literalmente en una encrucijada, y que un pequeño empujón en un sentido o en otro puede suponer un gran cambio en el resultado. Por ello, si la gente desea que los valores que promovemos tengan éxito, deberían apoyar a aquellas organizaciones e individuos que representan dichos valores, y empezar por promoverlos ellos mismos.

Scott: Yo añadiría: o convertirse en ellos.

Julian: Sí, o convertirse en ellos. Convertirse ellos mismos en la representación de esos valores. A mí siempre me ha dado reparo decir públicamente que todo el mundo debería salir ahí fuera y convertirse en un mártir, porque en realidad no creo en ello. En lo que sí creo es en que los activistas más efectivos son los que luchan y se retiran para seguir luchando en el futuro, no aquellos que luchan y se inmolan en el proceso. Es cuestión de juicio: hay que saber cuándo entablar pelea y cuándo retirarse para preservar recursos para la siguiente pelea.

Jared: ¿Dirías que luchar y retirarse no es tan diferente de luchar de forma anónima, mientras estés lo bastante seguro de que tu anonimato es sólido?

Julian: Si tu anonimato es perfecto, se puede luchar continuamente, sí. No hace falta huir.

Scott: Entonces has huido antes de tiempo.

[Risas]

Jared: En esencia, es eso: huir antes de tiempo.

Julian: Siempre se puede reducir el umbral del valor; es una de las cosas buenas que tiene el anonimato. Bueno, tal vez esa no es la forma de expresarlo. La gente me dice a menudo: «Eres increíblemente valiente al hacer lo que estás haciendo», y yo suelo responder: «No, tienes una idea equivocada de lo que es el valor. El valor no es la ausencia de miedo; solo los tontos no tienen miedo. El valor es más bien el control intelectual del miedo tras comprender los verdaderos riesgos y oportunidades de la situación, y mantener un equilibrio entre ambos». No se trata solo de saber cuáles son los riesgos, hay que ponerlos en práctica. Existen todo tipo de mitos por ahí sobre lo que se puede y no se puede hacer; lo importante es arriesgarse. Pero hay

que saber cómo hacerlo: uno no se pone a prueba saltando directamente desde un puente. Primero hay que saltar desde un taburete y después ir saltando desde sitios cada vez más altos.

Jared: ¿Puedo plantear otra cuestión sobre esto? Tiene que ver con lo que ha preguntado Scott acerca de la relación entre la persona que proporciona la información y la persona que la recibe. Si analizáramos las diferentes sociedades existentes en el mundo, probablemente veríamos que no todas tienen las mismas reglas de juego. Hay personas que simplemente tienen un mayor conocimiento de los riesgos asociados al uso de estas herramientas, y hay personas que pertenecen a sociedades con gobiernos más estrictos que otros. Parece lógico pensar que en países como Irán o Corea del Norte, donde se combinan regímenes muy controladores con poblaciones aún relativamente desconocedoras de estas herramientas y de los riesgos asociados a ellas, resulte casi imposible comprender los riesgos y oportunidades que antes mencionabas.

Julian: Pienso que son perfectamente capaces de aprender, como todos los demás. Estas sociedades están mucho más politizadas que las occidentales, y a la gente le gusta hablar de política cada noche mientras cena, por lo que no estoy muy seguro de que sea correcto mirarles con ojos occidentales y pensar que sencillamente no entienden la situación en la que están. Puede que los riesgos extrínsecos sean mayores, y puede que los demás riesgos asociados a realizar una actividad política sean también bastante altos, así que no hay que exagerar estos riesgos. Además, las posibles recompensas también son mucho mayores, pues pueden pasar a formar parte de un gran momento histórico. Y como solo vivimos una vez, todos corremos el riesgo de no haber vivido nuestras vidas al máximo; cada año no utilizado está desaprovechado al cien por cien.

Eric: Te voy a contar algo al respecto. Hace poco estuve con Warren Buffett, que tiene 78 años. Yo le dije: «¿Qué planes tienes para el futuro?», y él me respondió: «El próximo año será el mejor de toda mi vida», y yo dije: «Ya, claro…», pensando que obviamente me estaba tomando el pelo. Pero luego me di cuenta de que cuando tienes esa edad el año próximo siempre va a ser el mejor del resto de tu vida, porque en algún momento va a llegar un año que no va a ser tan bueno, y al final te vas a morir. Es genial, ¿no? El año que viene será el mejor de nuestras vidas.

[Risas]

LS: Julian, ¿te importa si saco algunas fotos para el libro? ¿Qué te parece si saco algunas de vuestra conversación? Por supuesto, las podrías ver. Tú decides. Podría sacar algunas desde aquí y otras desde ahí.

Julian: ¿Fotos de quién haciendo qué, exactamente?

Lisa: De vosotros, hablando. Solo de la conversación.

Julian: Oh, no hay problema.

Eric: Podemos usar mi cámara S95.

Lisa: Sí, exactamente. Se va a desarrollar toda una operación de alta tecnología aquí.

Julian: ¡No digáis nada antisemita durante los próximos meses!

Eric: Nosotros nunca diríamos nada antisemita.

Julian: No, no, lo digo porque que hace un tiempo vino un periodista ruso y se hizo una foto conmigo. Se llamaba Israel Shamir, tan judío como el que más, aunque se había convertido al cristianismo ortodoxo ruso y era bastante antijudaísmo. Publicó la foto en el *Russian Reporter* o algo así, y he tenido unos problemas increíbles por su culpa.

Eric: Interesante. Ambos sabemos los costes de la publicidad negativa.

Julian: Era una broma. Sé muy bien que tú también lo has sufrido.

Eric: Yo también lo he sufrido y por eso me porto bien. La crítica que se escucha constantemente es que todo lo malo ha ocurrido por culpa de WikiLeaks, pero yo aún no lo he visto. ¿Tienes alguna razón para…?

Julian: Bueno, es un truco retórico.

Eric: Pero entiendes por qué lo pregunto, ¿no?

Julian: Si, sí.

Eric: Intento comprender el motivo de la oposición a vuestra labor. Obviamente, nosotros os apoyamos totalmente.

Julian: Hasta la publicación de *Daño Colateral,* en Estados Unidos éramos una «cause célèbre» entre varios diferentes grupos; bueno, en realidad lo seguimos siendo, pero ahora solo entre comunidades de izquierdas o libertarias de derechas[237]. Según la agencia Reuters, en veinticuatro países contamos con el apoyo de más de las tres cuartas partes de la población. Nuestro peor porcentaje de apoyo está en Estados Unidos, con

aproximadamente el 40 %, lo cual no está nada mal, considerando todo lo que ha ocurrido.

La consecuencia de poner en evidencia a la clase militar y diplomática de Estados Unidos es que hemos sufrido un contraataque bastante significativo por parte de un grupo de poder que no solo se encuentra en la cúpula de la Casa Blanca, no son solo unos cuantos generales, sino que también incluye a toda la gente conectada con este sistema y que se beneficia del mismo. Esto incluye a un tercio de la población estadounidense, desde Chelsea Clinton hasta alguien de los barrios bajos de San Antonio que tiene un hermano destinado en Irak. Actualmente, en Estados Unidos hay unas 900 000 personas con acceso a información altamente confidencial[238], y cerca de dos millones y medio con acceso a información clasificada[239]; si consideramos los últimos veinte años y preguntamos cuánta gente ha tenido autorización para acceder a esta información, puede que la cifra ascienda hasta los 15 millones; y si incluimos todos los maridos y esposas, hijos y socios comerciales, estamos hablando de que en torno al 30 % de la población estadounidense está estrechamente relacionada con esa estructura ideológica y ese sistema de apoyo político. En Estados Unidos resulta muy difícil decir algo que vaya contra ese sistema, tal y como descubrió por las malas *The New York Times* cuando trató de pronunciarse al respecto; publicó material de WikiLeaks y tuvo que ponerse muy a la defensiva. Hasta los periodistas más tradicionales piensan que es repugnante ver como cualquier periódico alardea de lo «satisfecha» que está la Casa Blanca con su comportamiento[240].

Respecto a dichos ataques, siempre nos han acusado de haber «puesto en riesgo a las personas». ¿Riesgo con relación a qué? Ahora mismo corremos el riesgo de que un meteorito atraviese el techo de esta casa y nos mate a todos. Es un riesgo, sin duda, pero ¿es un riesgo lo bastante significativo como para mencionarlo? La respuesta es no. Ocurre lo mismo con la palabra «posibilidad»: existe la posibilidad de que un meteorito nos caiga encima en este preciso instante, pero la probabilidad es muy escasa. Las personas que esgrimen el tema de la seguridad a menudo se sirven de estos trucos retóricos: existe el riesgo de algo, o existe la posibilidad de algo. La gente debe defenderse contra esta manipulación retórica, y comprender que si alguien menciona que existe un riesgo sin especificar si ese riesgo es mayor que cruzar la carretera o que te pique una abeja, hay que ignorar a ese alguien. Y lo mismo ocurre con la cuestión de posibilidad frente a probabilidad.

Eric: Sí, yo pienso igual. ¿Hay algún ejemplo de un resultado positivo que pueda relacionarse directamente con WikiLeaks en la esfera política y que quieras destacar? ¿Algún resultado positivo explícitamente tangible?

Julian: Posiblemente el más significativo es la Primavera Árabe.

Eric: Dirías que WikiLeaks estuvo presente…

Julian: Lo ha dicho Amnistía Internacional en su último informe, igual que los activistas y académicos tunecinos**[241]**. Debido a mi implicación directa, no estaría bien que yo mismo lo dijera. De lo que estoy seguro es de que tuvimos cierta influencia y que nos involucramos profundamente.

Eric: Influisteis en ello.

Julian: Sin duda influimos en ello, y eso es algo importante en un gran momento histórico. Otra cosa de la que estoy seguro es de que cambiamos el resultado de las elecciones keniatas en 2007**[242]**, pues entre otras cosas pusimos en evidencia a muchos ministros que se vieron obligados a dimitir. Estas son acciones concretas y claras, aunque como se puede argumentar que fueron positivas o negativas en función de la opinión favorable o desfavorable de los afectados, tampoco quiero profundizar mucho en ellas.

Eric: De acuerdo, si retomamos tu anterior argumentación de que vuestro verdadero objetivo no es el efecto sobre un solo individuo, que el efecto real que buscáis es el cambio radical del sistema, porque la premisa principal es que este sistema se ha vuelto muy controlador y es estático e inmune a cualquier presión, entonces un ejemplo de influencia profunda sería una revolución, ¿no es cierto?

Julian: Sí, bueno, se puede tener una gran influencia sin necesidad de que se produzcan estos acontecimientos dicotómicos, pero estos acontecimientos —los acontecimientos binarios— son fáciles de discutir y de demostrar.

Eric: También tiene algo de *marketing*. La idea es tener una historia vendible.

Julian: Unas elecciones las gana un partido u otro, y eso es un cambio, un resultado muy claro. Si hay una revolución, primero hay un grupo en el poder y luego otro, y eso también es un cambio muy claro. En mi opinión, algunos de los otros cambios en los que hemos influido son más significativos, y posiblemente el más importante de todos aquellos en los que hemos participado es la liberalización del mundo editorial, algo que hemos

impulsado durante bastantes años[243]. Lo que hicimos el año pasado no habríamos podido hacerlo hace cuatro años; hubiera sido imposible.

Eric: ¿En qué sentido? ¿En términos tecnológicos o de…

Julian: Tecnológicamente era perfectamente posible. La diferencia la marcó un cambio en el *statu quo*: WikiLeaks se convirtió en el *statu quo*. Esto no fue siempre así: durante los dos primeros años luchamos por ser al menos aceptados en Internet. Después llegó el caso del Banco Julius Baer, por el cual nos vimos inmersos en un gran pleito legal en San Francisco[244]: por un lado estábamos nosotros, y por otro la entidad bancaria privada más grande de Suiza, el Banco Julius Baer, que intentaba clausurar nuestra página. Al final ganamos, y eso le costó su oferta pública de acciones en Estados Unidos[245].

Esto fue un signo claro de que en el mundo hay un sitio para editores como WikiLeaks, y con el tiempo hemos ido fortaleciendo nuestra posición en ese sitio. Actualmente ya tenemos unos cimientos muy sólidos, como lo prueba el hecho de que en octubre de 2010 el Pentágono ofreció una rueda de prensa de cuarenta minutos en la que su portavoz, Geoff Morrell, declaró que WikiLeaks —y yo mismo en particular— debía devolver todo la información perteneciente al Pentágono que habíamos publicado y toda la que nos proponíamos publicar, y dejar de solicitar información al ejército de Estados Unidos y al personal de su gobierno, pues de otro modo el propio Pentágono nos obligaría a ello. Cuando un periodista asistente le preguntó qué mecanismos utilizarían para obligarnos, la respuesta fue: «Bueno, mire, esto es el Pentágono; la ley no nos preocupa»[246].

Jared: Cuando viste ese vídeo, ¿pensaste que eran increíblemente ingenuos, que no eran conscientes de que la actual tecnología les haría imposible llevar eso a cabo?

Julian: Al principio tuve esa impresión, pero más tarde comprendí que lo que ocurrió en esa rueda de prensa fue algo más sofisticado.

Jared: Yo siempre tan poco sofisticado. Ja ja ja.

Julian: ¿Qué pasó en realidad? A primera vista parecía ridículo. ¿Por qué actuaba el Pentágono como una víctima? ¿Por qué daban una imagen tan ridícula e impotente? ¿Por qué amenazaban con algo que no podían cumplir? Les hacía parecer débiles. Pero en realidad se trataba de un mensaje legal cuidadosamente elaborado, diseñado para enredarnos en la Ley de Espionaje de Estados Unidos. Era una notificación, como la que se ve en los periódicos.

Eric: Exacto.

Julian: Exigimos que hagáis esto. Este es el tipo de información que puede causar un gran daño a la seguridad nacional de Estados Unidos. Convocamos una rueda de prensa para poder decir posteriormente que la gente de WikiLeaks era consciente de la amenaza, y que si WikiLeaks vuelve a publicar algo quedarán patentes sus intenciones. Pese a que advertimos a WikiLeaks de que no publicase, lo hizo de todas maneras, y por tanto sus intenciones son claras, porque no se pueden cometer actos de espionaje por casualidad.

Scott: Por eso les preocupa el pasado y no solo el presente, porque necesitan unas pautas de comportamiento, y mientras solo cuenten con ejemplos muy recientes no pueden encontrar esas pautas.

Julian: Sí, pero nos negamos rápidamente, antes de comprender cuál era la trampa legal. Y poco después publicamos los *Diarios de Guerra de Irak*, que es una de las mejores cosas que hemos hecho[247].

[Pausa en la grabación]

INTERLUDIO

[La grabación se reinicia en otra habitación]

Scott: …utilizando cada vez más la información de WikiLeaks como fuente, en ocasiones sin mencionar siquiera la propia fuente.

Julian: Bueno, al principio no nos citaban como fuente, pero ahora sí lo hacen. Ahora da más prestigio decir que procede de nuestra página.

Scott: Lo sé, lo sé, lo sé.

Julian: Curioso, ¿no?

Scott: Lo es, lo es, lo es.

Julian: Os voy a enseñar algo aún más curioso. ¿Os gusta nuestro eslogan?

Eric: Mantén la calma y sigue adelante, ja ja ja.

Scott: ¡La Segunda Guerra Mundial!

Eric: Estábamos admirando las fotos de los ancestros del dueño de la casa.

Julian: Estos son los ancestros de Vaughan. Y allí está mi amigo Vaughan en Afganistán, a principios de año.

Eric: Parece un reportero, ¿verdad?

Julian: Lo es. Reportero de guerra.

Scott: Disculpa, ¿quién es?

Julian: Es el dueño de esta casa, mi amigo Vaughan Smith.

Scott: Ah, vale, vale. ¡He estado en su club![248]

Julian: Sí, es reportero de guerra. Aunque en un principio perteneció a los Guardias Granaderos, creo que finalmente comprendió que podía ir a más guerras como reportero que como soldado.

Scott: Ja ja ja. Y a guerras muy diferentes. Es mejor así. ¿Es esta su familia?

Julian: Sí, todos estos son de su familia. Estos son sus padres, ambos viven en una casa en el otro extremo de la finca.

Jared: Entonces, es una familia con tradición militar.

Julian: La otra persona interesante es ese tío de ahí, Tiger Smith, el que lleva el cuello subido y tiene pinta de conquistador, famoso por haber matado 99 tigres en los tiempos en los que tal cosa aún gozaba de aprobación. El objetivo era salvar indios.

Jared: ¿Estaba relacionado con el Imperio?

Julian: Pues sí, esa es la parte curiosa: el padre de Vaughan fue mensajero de la reina.

Lisa: Oh, Isabel.

Julian: Iba en avión de aquí para allá para entregar todos los mensajes oficiales. ¿Veis esa bolsa que tiene en la mano? ¿Sabéis lo que había en esa bolsa?

Scott: Secretos de estado.

Julian: ¡Comunicados diplomáticos!

[Risas]

Eric: Es genial.

Julian: Tomaba a menudo el Concorde, y llevaba los asientos a su derecha e izquierda ocupados con bolsas llenas de mensajes y cosas para entregar; a veces, hasta llevaba ordenadores. Había agentes de seguridad que le acompañaban hasta el mismo avión para asegurarse de que no le robaban nada, y al aterrizar otros agentes le esperaban en la puerta del avión para recibir los envíos.

Lisa: ¿Y qué opina de todo esto?

Julian: Por un lado está aterrorizado, y por otro profundamente complacido, porque si le hubieran usado a él nada de esto habría ocurrido.

[Risas]

Eric: ¿Me permites preguntarte cuánto tiempo llevas aquí? ¿Seis meses?

Julian: Ocho meses ya.

Eric: Entonces esto es ya como tu casa.

Scott: Bueno, es un sitio realmente agradable.

Julian: Tengo que ir a la comisaría de policía todos los días.

Eric: ¿Está lejos?

Julian: A unos quince o veinte minutos. A menudo me tienden emboscadas. La más divertida de todas fue una mujer de Cataluña: se presentó en el Frontline Club, en Londres, e intentó convencerles de que era la principal programadora de WikiLeaks España.

Eric: ¡Ja ja ja ja ja!

Julian: Y claro, como allí nadie sabía lo más mínimo de programación, a esta mujer le bastó con usar un poco de tecnojerga para que la creyeran, aunque le dijeron: «Eh, en realidad no puede ver a Julian, porque está aislado», y la alojaron gratis una noche. Esta mujer tenía la costumbre de escuchar cualquier conversación e incorporarla a su historia, por lo que al día siguiente empezó a decir: «Oh, a ese le conozco; oh, mira, ahí está fulanito».

Eric: Ja ja ja.

Julian: Entonces, dos semanas más tarde la policía entró en esta casa y me dijeron: «¿Conoce a X?»

«¿X? ¿Quién es X?»

«¡Su novia!»

[Risas]

«No»

«Pues ha estado toda la noche en una casa en el límite de esta propiedad, y dice que usted pagará la factura del taxi».

[Expresiones de asombro]

Y yo dije: «¿Qué factura de taxi?» Resultó que, tras volar de Cataluña a Londres, allí había tomado un taxi hasta aquí: una carrera de 500 libras, y ella solo tenía 50, pero convenció al taxista de que su «rico y famoso» novio pagaría la factura. Tuvieron sus más y sus menos, pero quedaron en que todo se arreglaría. Fueron al límite de la finca, ella dijo que era mi novia, y el taxista no quería irse, porque quería su dinero. Los vecinos de la propiedad les acogieron por esa noche.

[Risas]

Scott: ¿En qué momento le pagaste por su creatividad?

[Risas]

Eric: ¡Aunque solo sea por el espectáculo!

Scott: Es todo tan creativo que es hasta impresionante.

Eric: No quiero abusar de tu energía ni de tu tiempo. Creo que sería interesante hablar un poco de los distintos escenarios hipotéticos. Esto nos interesa mucho; Jared y yo pensamos en ello continuamente. ¿Qué escenarios podrían desarrollarse? Ya sabes, intentar imaginar realmente cómo serían. Tienes muchos actores y figurantes, y obviamente piensas mucho en ello. En la práctica eres como un físico, ¿no? Piensas de esa forma.

Julian: Tal vez deberíamos ir a dar un paseo.

NO ES FÁCIL HACER WIKILEAKS

[Caminando sobre empedrado]

Jared: A la hora de plantear escenarios hipotéticos, puede resultar realmente útil plantearlos en el pasado. Por ejemplo, uno de los capítulos de nuestro libro trata sobre la intervención en el contexto de un genocidio futurista; pero para entender el papel que WikiLeaks podría tener en una situación como esta, tal vez sea más útil preguntarse qué hubiera pasado si durante el genocidio de Ruanda en 1994 WikiLeaks hubiese existido y la tecnología de entonces hubiese sido igual de avanzada que la de hoy en día: ¿Qué habría cambiado?**[249]** ¿Qué aspectos podrían haber sido diferentes?

Julian: Ahora mismo, lo único que me pregunto es cuándo cambiará el tiempo.

Jared: Bienvenido al clima británico. Ja ja.

Eric: Bueno, la nube se acabará moviendo.

Julian: El genocidio en Ruanda. Sí, pienso que si hubiesen tenido Internet y teléfonos móviles, la situación hubiese sido algo diferente; cuando menos, se habría sabido más sobre el tema. Aunque la verdad, lo más probable es que tampoco hubiese supuesto gran diferencia, porque por ejemplo lo que está pasando ahora en el Congo no está teniendo mucha repercusión en Occidente que digamos.

[Empieza a llover]

Scott: Ahí tenemos un magnífico árbol, que nos mantendrá totalmente secos.

Julian: Estupendo.

Jared: En relación con lo anterior, tengo una hipótesis. Bueno, en realidad, parte hipótesis y parte pregunta: ¿por qué en países como Irán, Corea del Norte o Congo no ha habido gente que publique documentación al respecto, igual que ha existido en las democracias occidentales?

Julian: Bueno, en realidad tenemos alguna información sobre Irán**[250]**. No es tan fácil hacer WikiLeaks: la combinación de aspectos técnicos, reputación, financiación, etcétera. No es nada fácil.

Scott: Para empezar, la reputación es muy difícil de conseguir.

Eric: Está bien, pero hagamos la pregunta sin tapujos: ¿Por qué no estáis recibiendo una enorme cantidad de *pendrives* sobre los países africanos con malvados dictadores?

Julian: Sí que lo hacemos.

Eric: ¿No crees que todo el mundo podría estar interesado en utilizaros como difusor? ¿No deberían estarlo?

Julian: Hemos recibido algunos documentos bastante decentes sobre África y Timor Oriental, y muchos sobre América Latina[251].

Eric: ¿Esto se debe a que estos gobiernos no documentan tanto estos temas?

Julian: No están tan conectados a la red. Algunos de ellos no tienen el inglés como idioma oficial; el gobierno de Tanzania, por ejemplo, utiliza el swahili. Su participación con nosotros tiene mucho que ver con si consideran o no a WikiLeaks como un actor político dentro de su país. Una vez que conseguimos un poco de información sobre Timor Oriental, empezamos a conseguir mucha más y al final se acabó creando un enorme flujo, por lo que actualmente ya recibimos documentación de forma rutinaria; pero para ello tienen que percibir que somos parte de la comunidad. En el caso de Rusia, aunque recientemente hemos creado RuLeaks, que no lo está haciendo nada mal, creo que la escasa cantidad de material que hemos publicado en realidad es una señal positiva, pues supone que la esfera de Internet rusa es muy activa por sí misma[252].

Eric: Sí, acabo de estar por allí. Es increíble.

Julian: La verdad es que no miran mucho lo que hay fuera. ¿Por qué iban a visitar una página en inglés como WikiLeaks? Allí tienen sus periodistas activistas sin ánimo de lucro y su oposición, y todos están dentro de esa esfera de Internet, que es relativamente libre comparada con la televisión rusa, así que no ven la necesidad de escoger esta otra avenida.

En un momento dado se publicaron un montón de documentos del SFS en un servidor estadounidense, pero la publicación fue inmediatamente intervenida y nunca más se volvieron a ver esos documentos[253]. No es tan fácil publicar en contra organismos estatales tan poderosos.

Jared: Has hablado mucho sobre la importancia del nombre y ha sido un tema importante en nuestra conversación. Por un lado está el debut de una página, el momento en el que pasa a estar activa, y después está el gran debut,

en el que se convierte en un nombre y en una página de uso diario, y una de las cosas que estamos considerando en el libro…

Julian: Aún no hemos llegado a ese nivel. No hemos sido capaces de hacer crecer la página tan rápido como su nombre.

Jared: La gente sabe lo que es WikiLeaks, y me pregunto si en el caso de que la primera remesa de documentos hubiese procedido de, por ejemplo, Irán o Corea del Norte, y se hubiese publicado, ¿el mundo la hubiese considerado como una plataforma de información clandestina?

Julian: ¡Así fue![254] El mundo lo consideró así hasta que empezamos a publicar un gran volumen de información militar de Estados Unidos. En 2007 publicamos miles de páginas de documentos militares[255].

Eric: Y nadie se dio cuenta.

Jared: Eso es interesante.

Eric: Porque el vídeo *Daño Colateral* aún no había salido a la luz.

Julian: Lo que publicamos sobre Guantánamo se difundió bastante, pero no hasta el punto de que WikiLeaks se convirtiese en un nombre conocido entre la gente de a pie. Entre los periodistas nos convertimos en un nombre conocido con bastante rapidez, igual que entre la parte técnica de la comunidad pro-derechos humanos. Y también nos hicimos un nombre entre los usuarios habituales de Internet germano y angloparlantes, especialmente en el sector de la criptoseguridad: por ejemplo, cuando hicimos una campaña de recaudación de fondos entre enero y marzo de 2010, antes de *Daño Colateral*, conseguimos un millón de dólares. El hecho de que un nuevo —nuevo en términos de concepto— grupo periodístico, sin ánimo de lucro, obtenga un millón de dólares en donaciones de veinte dólares es algo casi absolutamente inaudito. E insisto en que esto lo logramos antes de *Daño Colateral*.

Lo cierto es que ni siquiera *Daño Colateral* nos convirtió en un nombre conocido en todo el mundo, solo en Estados Unidos, pero a finales de ese año las cosas empezaron a precipitarse. Curiosamente, fue el ataque del Pentágono contra nosotros y el caso del acoso sexual en Suecia el que finalmente nos dio a conocer a nivel mundial, con un reconocimiento del 84 % en todo el mundo[256].

Eric: Eso es interesante. Entonces, si asumimos que la situación legal actual se acabará resolviendo, los próximos años son… ¿Qué ocurrirá con

WikiLeaks? Para nosotros, el punto de partida será el próximo año; así que estamos hablando de dentro de un año, el año que viene. ¿Se hará WikiLeaks más grande, con más donantes y más tecnología? ¿Vais a cambiar de alguna forma?

Julian: Hay muchos cambios previstos. Pienso que mi idea sobre cómo estructurar la información intelectual es importante y que la aplicaremos.

Eric: Entonces, ¿es eso parte del plan?

Julian: Sí. Cuando cuentas con semejante reconocimiento público, puedes permitirte el lujo de concebir ideas intelectuales bastante complejas —ideas a las que normalmente llevaría mucho tiempo tomar impulso con el solo apoyo de la organización— y ponerlas en práctica, como hizo Sun con Java, por ejemplo[257]; podemos apuntalar bien una idea y levantarla. Pero también vemos que nos resulta difícil ser una organización basada en las órdenes y el control. Antes habéis hablado de las dificultades que tuvisteis para aprender con Novell, pero nosotros como organización estamos en una posición en la que tenemos a toda una superpotencia, con sus organismos de investigación, y al resto de la OTAN operando contra nosotros, sobornando a la gente, controlando nuestras conversaciones, etcétera[258]; esto implica que la más mínima debilidad psicológica de nuestra gente o cualquier fricción entre ellos puede hacer que estas fuerzas acaben con nosotros.

Eric: Oh, en teoría incluso podrían infiltrarse.

Julian: Sí. En mi opinión, perseguir a los empleados es un problema mayor, pero tienes razón sobre la infiltración.

Eric: Pero esas fuerzas que se os oponen pueden pensar: «A ver, este es un extranjero; enviemos a nuestro agente, para que se haga miembro de su organización y descubra todos sus secretos».

Julian: Eso es cierto; somos conscientes de este riesgo y por ello investigamos a las personas. El problema es que esto ha ralentizado muchísimo nuestro crecimiento, porque no podemos simplemente poner un anuncio diciendo que necesitamos a personas con determinadas habilidades y que los interesados deben presentarse en nuestras oficinas; eso es completamente imposible, por lo que nuestro crecimiento se ve restringido. Sin embargo, hay otra forma de liderazgo, y es utilizando valores, en lugar de órdenes y control. Cuando lideras mediante valores no es necesario confiar en la gente, y no está limitado ni el número de personas que pueden adoptar estos

valores ni la velocidad a la que se pueden adoptar. Todo sucede muy rápido. El sistema no está limitado por la oferta —en términos de oferta de empleados— sino que más bien está limitado por la demanda: la gente puede adoptar un valor tan pronto como lo demandan.

Eric: Ya veo. Para mí esto significa que el poder de una idea está infravalorado, y que si logras implantar correctamente una idea la comprarán millones de personas. En mi opinión, las ideas más profundas que has señalado o bien no son comprendidas o tienen que luchar contra la desinformación. Como has dicho, es un uso inteligente de las palabras que se vuelve en tu contra o algo así. Os enfrentáis al reto de conseguir que los argumentos más profundos que nos has planteado se escuchen a pesar de las fuerzas que trabajan en contra.

Julian: Si cuentas mentiras durante el tiempo suficiente, la gente comienza a creérselas. «El comunicado sobre Afganistán fue algo terrible»; esto se difundió tan rápidamente que hemos renunciado ya a intentar desmentirlo. Hay otras cosas en las que vale más la pena gastar energías, aunque estamos intentando informar a una gran variedad de personas acerca de nosotros, nuestros valores y aquello en lo que creemos. Lo que está ocurriendo es que esta gente, a pesar de estar distribuida en muchos países de todo el mundo, se está comunicando entre sí. Estamos creando nuestra propia red informática de personas que piensan de la misma forma, y que pueden confiar el uno en el otro en los puntos básicos. Comenzamos el año pasado en una posición en la que tuvimos un gran enfrentamiento con el Departamento de Estado y el Pentágono al mismo tiempo. ¡Uno de nuestros mayores éxitos es que hemos logrado que el Pentágono y el Departamento de Estado cooperen en algo!

[Risas]

Tienen una gran organización interna; tienen sus listas de contactos; tiene un sistema de correo electrónico interno; tiene su estructura de órdenes y control para asignar tareas a las personas y asignar recursos a estas tareas; y tienen personal disponible para dedicarlo a nosotros, tal vez unas 10 000 personas. En este caso concreto, estos son nuestros enemigos. Por otro lado, nosotros tenemos millones de personas de todo el mundo que nos apoyan y apoyan nuestros valores, personas que normalmente están completamente desperdigadas. Para ellos no existe una estructura de órdenes y control, por lo que entre otras cosas no pueden coordinarse de forma efectiva. Esa es la situación inicial pero, a medida que esta gente se va encontrando a nivel local,

comienza a formarse una organización. Y a medida que se van conociendo mutuamente, la organización se va optimizando: la red de nodos empieza a crear vínculos, volviéndose cada vez más eficiente a la hora de entender su entorno, planificar sus acciones y llevarlas a cabo. Tenemos planes para potenciar eso. Vamos a tomar estos gráficos de varios millones de simpatizantes y… ¿sabéis qué es el recocido simulado?

Eric: No.

Julian: Cuando alguien hace una aleación, se tienen dos metales diferentes y la idea es crear un solo metal a partir de esos dos. Para ello, se mezcla uno con otro y las moléculas de ambos metales se disponen entre sí de manera que la atracción entre ellas sea máxima, y la energía mínima. Lograr esto puede ser bastante difícil, porque una molécula puede estar asociada a otra situada a su izquierda, pero la disposición más sólida es aquella en la que se asocia a otra molécula a su derecha, por lo que necesita un proceso que le haga abandonar un vínculo y establecer otro. Este proceso se llama recocido. La gente que fabrica estas aleaciones funde los metales, los mezcla y los deja enfriar conjuntamente un poco, luego los calienta otro poco, luego los enfría y luego los vuelve a calentar, siempre poco cada vez; incluso pueden llegar a golpear la mezcla de diferentes formas. Pues bien, estamos desarrollando un sistema en el que metemos a toda esta gente en una red que después templamos con un método de recocido o templado simulado, de forma que se cree el vínculo más sólido posible entre estos millones de personas.

Eric: Alrededor de un conjunto de principios.

Julian: Alrededor de un conjunto de principios que los unen.

Eric: Entiendo.

Julian: Y entonces tendremos una red informática eficiente —en términos humanos— a la que podremos observar, y planificar y actuar sobre ella.

PUBLICACIÓN TOTAL

Eric: Otra crítica, creo, con respecto a WikiLeaks: según los informes, trabajasteis con sumo cuidado en la redacción de información sensible. Tal y como yo lo entiendo, hubo un proceso de edición, alguien tuvo que crear un motor de búsqueda especializado porque los documentos eran muy

complicados, hubo un periodo de revisión bastante extenso con los medios de comunicación, etcétera. Todo esto está bien documentado. Ahora bien, imaginemos que existen otras personas que no son de vuestro grupo, que no comparten los mismos valores pero que tienen la misma tecnología, porque obviamente la tecnología es imitable: ¿qué pasa cuando ellos son más que vosotros? ¿O al menos los mismos?

Julian: Bueno, ¿quién controla a WikiLeaks? Nosotros tenemos nuestros valores, pero ¿cómo sabe la gente si los cumplimos o los traicionamos? Puede haber gente a la que no le gustan nuestros valores, y puede haber gente a la que sí le gusten. ¿Cómo puede el ecosistema económico humano disciplinarnos o alentarnos a avanzar en determinadas direcciones?

Las fuentes hablan por sus acciones. Si estas fuentes saben que las vamos a proteger y que con nosotros su material va a tener un gran impacto, sencillamente nos lo darán a nosotros en vez de a algún otro. Esta es una de las formas que tiene el mercado de fuentes para disciplinarnos.

Eric: Entonces hay una especie de sesgo de selección.

Julian: La cuestión es: ¿estas fuentes podrían escoger a otro grupo para publicar su material aunque no disponga de un procedimiento de minimización de riesgos? La respuesta es sí, pero hay que entender la razón principal por la que llevamos a cabo estos procedimientos. No lo hacemos porque la documentación publicada, al revelar información sensible, puede conllevar un riesgo razonable de producir un daño real fruto de la revelación, ya que eso muy rara vez ocurre. En realidad, lo que sí es bastante probable es que, si no aplicamos este procedimiento, nuestros oponentes intentarán, de manera oportunista, desviar la atención de las revelaciones publicadas —cuestiones muy importantes— insistiendo en la posibilidad de un daño potencial, y por tanto en la posibilidad de que la publicación resulte contraproducente —puesto que lo que queremos es promover la justicia— y de que la organización sea hipócrita. Por ello, muchos de los procedimientos que llevamos a cabo no solo van dirigidos a intentar minimizar el riesgo que puedan correr las personas nombradas en el material, sino que también se trata de minimizar el riesgo de que los oportunistas reduzcan el impacto del material publicado. Así pues, parte del proceso de maximización del impacto que llevamos a cabo es para evitar este tipo de ataques contra lo que publicamos. De este modo, las fuentes comprenderán que lo que hacemos tiene el objetivo de maximizar el impacto. Dicho esto, nosotros no censuramos nunca lo que nos llega. Lo que hacemos es retrasarlo: lo

retrasamos hasta que la situación cambie y podemos publicar la información recibida.

Eric: Entonces, ¿puede decirse que incluso la documentación censurada acabará siendo publicada tarde o temprano tal y como estaba?

Julian: Sí.

Lisa: Pero en realidad esto no es lo que te estabas preguntando, que era qué pasaría si los mismos procesos y tecnologías cayeran en…

Julian: Sí, ahora llego a eso. Tenemos todo tipo de proyectos para sindicar nuestro sistema de protección de terceras personas. Me preocupa que no estemos protegiendo nada. Es un terreno muy resbaladizo, y ya he dicho que esto lo hacemos no solo para minimizar daños, sino también por motivos políticos, para impedir que algunas personas intenten desviar la atención de la parte importante de lo publicado centrándose en los posibles riesgos.

Jared: Es una decisión pragmática, una decisión estratégica.

Julian: Es una decisión pragmática y táctica para mantener el máximo impacto y no permitir que la atención se disipe; pero, aquí ya nos estamos metiendo en un compromiso bastante peligroso, aunque desde luego no tanto como lo hacen los periódicos. Hemos colaborado con ellos y hemos visto que algunos de ellos son sencillamente espantosos; incluso llegamos a publicar un análisis comparativo del contenido de algunas de sus redacciones con lo que realmente debía ser publicado, y el resultado es extremadamente interesante[259].

Eric: ¿Entonces había discrepancias sobre lo que debía ser censurado?

Julian: *The Guardian* censuró dos tercios de un documento sobre el crimen en Bulgaria: eliminó todos los nombres de los mafiosos que se habían infiltrado en el gobierno búlgaro[260]; eliminó la parte de la descripción de la élite de Kazajistán, en la que se afirmaba que la corrupción de esta élite era generalizada (no mencionaba nombres concretos, simplemente decía que la corrupción era general); y eliminó la descripción como corrupta de una compañía energética italiana que operaba en Kazajistán[261]. Así pues, censuraron la aparición de nombres de personas que podrían quedar expuestas y en peligro, igual que hacemos nosotros (es lo que les requerimos); censuraron los nombres de los mafiosos, porque les preocupaba que les denunciasen por difamación; y censuraron las descripciones de compañías supuestamente corruptas porque no querían exponerse al más mínimo riesgo.

Y esto ocurre también en el *Irish Independent*, a pesar de ser un excelente periódico y que sus periodistas son totalmente legales. En todas partes existe una increíble autocensura, y nadie reconoce llevarla a cabo ni revela el hecho de que la está llevando a cabo. WikiLeaks no quiere ir por ese camino. Estoy seguro de que todas estas instituciones comenzaron diciendo: «No, simplemente vamos a hacer estas pequeñas modificaciones», y luego entró en juego la economía, y pensaron: «¿Por qué arriesgarse?». Al final se acaba teniendo un sistema de autocensura, y es algo muy embarazoso, así que ¿por qué revelar al público que lo están haciendo?**[262]** Si no se dice nada, cada vez se vuelve más y más fácil hacerlo**[263]**.

El correo electrónico: nadie lo censura. Una llamada de teléfono a tu abuela: ¿acaso hay un censor en línea para decidir si hay riesgo de que le digas algo malo a tu abuela para cortar la comunicación? Claro que no. El correo postal: ¿hay gente abriendo sobres para ver si envías algo malo? No. YouTube: *a priori*, ¿hay alguien que revise cada vídeo antes de que se suba a la red?

Eric: Déjame darte la respuesta técnica, para asegurarme de que la sabes. No podemos revisar cada vídeo, así que es básicamente el público quien lo señala si lo consideran un problema.

Julian: ¿Sí? ¿Pero después de la publicación?

Eric: Después de la publicación.

Julian: Entonces, una vez publicado, cualquiera podría hacer una copia y difundirlo por todas partes.

Eric: Y lo que ocurre es la eliminación de… Tenemos problemas porque bastantes usuarios nos piden que revisemos los vídeos antes de su publicación, pero como cada minuto llegan a YouTube cuarenta y ocho horas de vídeo, es materialmente imposible verlo todo. Así que si alguien sube algo pernicioso, subversivo o ilegal, sea lo que sea, siempre transcurre un periodo de tiempo, con suerte corto, entre el momento de la publicación y aquel en el que se señala para ser revisado, conforme a nuestras normas. Normas que están claramente detalladas en un documento.

Julian: Si.

Lisa: No obstante, el criterio para eliminar algo es bastante estricto. Por ejemplo, no se eliminan vídeos simplemente porque expongan hechos erróneos.

Eric: Pero tal y como funcionan estas cosas, las páginas web comerciales, podemos decidir qué queremos permitir y qué no. Tenemos una serie de criterios que se pueden ver y se pueden leer. Queremos algunos tipos de vídeos, y otros no los queremos, y no se puede violar el *copyright* y todo eso.

Julian: Me gustó bastante lo que ocurrió con *Daño Colateral*: nuestros oponentes lo clasificaron inmediatamente como material para adultos, por lo que nadie podía verlo directamente en YouTube sin registrarse, y sin embargo se podía ver perfectamente si estaba insertado en cualquier otra página[264]. Mi interpretación de todo esto es que cuando un vídeo está insertado, la responsabilidad es de otros, ¡pero si no lo está, es la marca Google la que asume la responsabilidad![265]

[Risas]

Eric: Sin conocer los detalles específicos, todo cuanto puedo decirte es que el sistema responde a los comentarios de los usuarios tras la publicación. En YouTube ha habido algunos casos en los que se han producido fraudes en la valoración: por ejemplo, Jared publicaba un documento y alguna gente decidía que quería tumbarlo; como estaba siendo atacado, le daban un montón de puntos negativos y en consecuencia su puntuación pasaba a estar muy por debajo de lo que debería. Estos sistemas pueden ser manipulados por grupos de presión, y en mi opinión en este caso esto podría ser una constante.

Jared: A veces son los propios gobiernos los que lo hacen: hay algunos regímenes autocráticos que señalan como inapropiado el contenido publicado por los activistas.

Julian: Muchas cosas de las que hemos publicado han sido marcadas, y lo mismo les ha ocurrido a los oponentes de la Cienciología. Creo que unos 5000 vídeos contra la Cienciología fueron eliminados de YouTube cuando algún abogado juró que todos ellos le pertenecían[266] y que infringían su *copyright*.

Como la temática del material que nos llega es casi estrictamente política —y no me refiero a los partidos políticos, sino al ejercicio del poder— actualmente estamos sometidos a tal escrutinio que si pasásemos al sistema de publicar primero y retirar después nos dirían: «¡Demasiado tarde! ¡Ya lo habéis dado a conocer y ahora ya hay más de mil copias por ahí!»

Eric: Vosotros tenéis un sistema diferente. Utilizáis editores humanos.

Julian: Pero es un serio problema, porque implica que nos resulta muy difícil expandirnos. Por ello ahora utilizamos un sistema de subcontratación que consiste en externalizar la edición a organizaciones sin ánimo de lucro o similares.

Eric: Pero en esencia lo que estáis subcontratando es el juicio humano, porque hoy en día no es posible escribir algoritmos informáticos que hagan esto por ti.

Julian: La publicación sin investigación previa tiene un coste, pero lo cierto es que las dificultades de revisar antes de publicar son tan serias que suponen un problema muchísimo mayor. Si hay que elegir entre ambos, lo mejor es la publicación sin revisión.

Eric: Eso también nos interesa. Implica que en la práctica preferís… Estás tan preocupado por el juicio humano y la posibilidad de un sesgo…

[Interferencias del viento]

Julian: La idea es pedir a la fuente que se encargue de ello; pasaríamos el peso de la edición a la gente que nos entregue el material: «Debéis aplicar vuestro buen juicio sobre lo que nos enviáis, porque todo lo que nos enviéis lo vamos a publicar». De otro modo nos pondríamos en peligro, pues cuando otras personas comprendiesen que tenemos un mecanismo para determinar qué se publica y qué no, iban a intentar atacar ese mecanismo.

Jared: Bueno, en realidad tengo una pregunta sobre eso. Rebobinando, estamos hablando del futuro, de cada uno de los aspectos del libro, y lo que me pregunto es: ahora mismo estáis recibiendo un determinado volumen de documentación, y al igual que Twitter, que en un momento tuvo también demasiado contenido, llega un punto en que la información es tan abrumadoramente grande que si publicas todo lo que recibes existe tal mezcla, hay tanto contenido manipulado que el contenido legítimo en esencia se pierde…

Julian: El contenido manipulado nunca será un problema, aunque hay que decir que es importante tener un archivo inmaculado, como tenemos ahora mismo. Pero la parte manipulada siempre será una parte insignificante de todo el material, y esto se debe a que la manipulación requiere esfuerzo económico, y para llevarla a cabo se necesita a alguien aún más inteligente e informado que la persona que creó el documento original. Y si se va a

publicar todo el documento, la situación no es la misma que si se publica una noticia en la que uno se limita a dar al periodista contenido manipulado; hay que engañar también a tus oponentes y a todo el resto del mundo, lo que obviamente es mucho más difícil. Además, cada organización genera montones de papeles y registros internos simplemente llevando a cabo sus actividades, por lo que todos esos registros se producen de forma gratuita. El contenido legítimo siempre será mayor que el manipulado; el problema es que una pequeña cantidad de contenido manipulado puede devaluar una cantidad mucho más grande de contenido no manipulado.

Eric: ¿Puedo discrepar contigo en un punto? Estoy convencido de que la desinformación se va a convertir en algo muy fácil de generar, porque la complejidad va a ahogar al conocimiento, porque en cierto modo a determinada gente, le va a interesar crear sistemas generadores de desinformación durante la siguiente década. Es el caso de las corporaciones, de la mercadotecnia, de los gobiernos, etcétera. Todo lo cual hace que el trabajo de los «auténticos» periodistas sea mucho más difícil, ¿verdad? Y tu respuesta de antes era que básicamente se trata de un problema de confianza, cosa que en mi opinión se aproxima bastante a la verdad. Yo diría que se trata sobre todo de un problema de valoración: las valoraciones se basan en la confianza y en otros algoritmos; es la misma conclusión. Pero, desde mi punto de vista, no es cierto que siempre vaya a haber más información verdadera que manipulada, pues es perfectamente factible que los ue estén interesados se den cuenta de que los sistemas informáticos de IA pueden generar mucha información falsa[267]. Creo que estás al corriente de los proyectos que apuntan a que los ordenadores serán capaces de redactar documentos por sí solos.

Julian: Sí, los he visto. Siempre ha habido gente que ha pensado que estos ordenadores inundarían el mercado, y por ahora nunca ha ocurrido. Si excluimos a los chiflados que van contando por ahí cómo una noche, hace doce años, hablando con su exmujer a través del follaje de una gran maceta, ella le dijo que él era el Anticristo, y el comprendió que era verdad…

[Risas]

Si se excluyen esos casos, que son bastantes, han existido unos veinte intentos genuinos de fraude. Es extraordinario, son realmente pocos.

Eric: No, y además podrías argumentar que este hecho pone de manifiesto que el altruismo y la bondad existen, y que los pasos requeridos para

manipular de verdad son tan difíciles de dar que quien los diera tendría que tener intenciones realmente malas. El listón a superar está bastante alto.

Julian: ¿Y cuál es el que se acerca más? El fraude de inflar y tirar en el mercado de acciones, por ejemplo[268]. Es el que más solemos ver, sobre todo en forma de GIF[VII], e incluso tienen dispositivos para eludir el reconocimiento OCR en los correos electrónicos[269].

Eric: En el caso de Google, vemos montones de grupos de enlaces que intentan manipular nuestros *rankings*. Y los detectamos.

Julian: Bank of America llegó a solicitar a HBGary, un contratista de inteligencia de alta tecnología, que hiciese una oferta para desmantelarnos[270]. Conseguimos hacernos con una copia de la oferta, y aunque no sabemos quién acabó consiguiendo el contrato, el presupuesto era de 2 millones de dólares al mes, y con él podían difundir desinformación, piratear y atacar a nuestros periodistas; también dispondrían de mapas de las redes de personas que nos apoyan para enfrentar sus carreras e intereses con su ideología. Eso es lo que hay, pero la desinformación siempre ha estado ahí. No tengo muy claro por qué el aumento de información que estamos viendo en todas partes habría de llevar aparejado un incremento de la desinformación.

Eric: Por cierto, este es un argumento básico contra algo de lo que hemos hablado hace un rato. Es preciso que lo resolvamos de alguna forma.

Scott: ¿Qué tal echando un pulso?

[Risas]

Jared: Lo cierto es que este es uno de los más interesantes… Toda la conversación ha sido fascinante, pero esto último es especialmente fascinante por que tiene que ver con lo que Eric, Scott y yo estamos pensando para estos capítulos. Imaginemos la situación de aquí a diez o quince años… Bueno, por concretar, imaginemos que dentro de diez años no solo a los grandes grupos les resulta muy fácil crear documentos falsos, producirlos y distribuirlos en masa, sino que un solo individuo tiene esa capacidad, gracias a las plataformas tecnológicas que tienen a su disposición.

Julian: No veríais a Julian Assange decir que eso es cierto

Eric: [Julian] está planteando un argumento más importante: está diciendo que la humanidad no se organiza de esa forma. Las barreras que los valores

éticos de las personas, por así decir, ponen a la hora de actuar para hacer todo eso, tienden a limitar la cantidad de actuaciones, pues de otro modo ya se habría hecho muchas veces.

Jared: Imaginemos un gobierno entonces; ¿cuál tendría motivos potenciales para hacer algo así?

Julian: Es que actualmente ya hacen todo eso. El brazo de propaganda y comunicación estratégica del Pentágono cuenta con un presupuesto de unos 6000 millones de dólares al año[271].

Scott: ¿Pero alguien lo ha hecho utilizando vuestra página? En otras palabras, un gobierno contra otro gobierno utilizando WikiLeaks como lavandería.

Julian: No nos importa mientras sea la verdad. Si se trata de información verdadera, no nos importa de donde proceda. Si la gente lucha con la verdad, cuando se retiren los cuerpos habrá balas de verdad diseminadas por todas partes, lo cual es positivo.

Scott: Pero eso plantea de nuevo el tema de la capacidad de vuestra editorial de verificarlo todo.

Jared: Cierto, porque no es lo mismo eso que decir simplemente que publicaremos todo.

Scott: Es un terreno resbaladizo diferente, pero sigue siendo un terreno resbaladizo.

Julian: No, yo creo que no lo es en absoluto. Pienso que ese es el verdadero objetivo: dejar que la gente luche con la verdad.

Eric: Pero el argumento en este caso es que tiene que haber un algoritmo alternativo, que tienes que poder saber de alguna forma que estás tratando con una fuente legítima y que la fuente puede elegir al editor.

Scott: No, entiendo lo que dices, pero esa es la razón por la que la ecología está en contra de toda sociedad en la que no se puede verificar nada: la gente se queda sola, y WikiLeaks no puede ayudarla; solo puede decir: «Cuando tengáis un buen sistema de verificación, hablamos; de otro modo, buena suerte».

Lisa: Pero lo que están verificando son documentos, no hechos.

Jared: No, lo que verifican son las fuentes.

Julian: No, no, no verificamos las fuentes, verificamos que los documentos sean oficiales.

Lisa: Eso, documentos oficiales.

Scott: Aun así, en parte verificáis las fuentes.

Lisa: Pero no los hechos, por lo que no se trata de perseguir la verdad.

Julian: No se trata de verificar los hechos, es cierto.

Scott: Bueno, eso es otro debate. Ja ja ja. ¡Se trata de verificar los documentos, no de verificar la verdad!

Jared: Eso nos lleva otra vez al tema del ruido, ¿no? La tecnología no solo genera ruido en el contexto de una revolución. En el futuro habrá que enfrentarse a más ruido, y la cuestión no es si los seres humanos prefieren la verdad a la ficción, sino si pueden encontrar la verdad y distinguirla de la ficción.

Eric: Es que ese es el quid de la cuestión. Él no está de acuerdo conmigo en este punto, y tenemos que resolver la discrepancia.

Julian: Hemos publicado todos los documentos falsos que han llegado a nuestras manos que nos han parecido interesantes, pero los hemos publicado advirtiendo de que eran falsos.

Jared: ¿Ahora sois WikiFalsificaciones[VIII]?

Julian: Pero no es para tanto: en realidad, no son falsas; en un meta nivel, son verdaderas falsificaciones.

Eric: Son realmente interesantes en sí mismas y por lo que suponen, ¿verdad?

Julian: Sí, muy interesantes en ambos niveles. Una de ellas fue un intento de influir en las elecciones de Kenia diciendo que la oposición había firmado un acuerdo secreto con la minoría islámica para introducir la ley islámica en todo el país[272]. Suena ridículo, pero fue algo cuidadosamente elaborado.

Jared: ¿Cómo supisteis entonces que era una falsificación?

Julian: Bueno, ese caso fue difícil, porque como digo era un documento redactado con gran cuidado. Lo que hicimos fue comprobar las firmas y encontramos la verdadera. Fue un trabajo complicado, aunque normalmente no lo es.

Jared: Pero requiere recursos humanos para llevarlo a cabo, ¿no?

Julian: Sí. Normalmente, suele haber alguien que comente un error elemental. Hay pocos incentivos en mandarnos a nosotros una falsificación, porque se nos considera bastante buenos a la hora de detectarlas, y además publicamos la totalidad del documento. Así es que las suelen mandar a algún periódico, porque no publican todo el documento y no tienen nuestra capacidad en ese campo. Es mucho más fácil engañarles a ellos.

La cuestión de la que hablas… digamos que vosotros no tenéis verificadores como nosotros. La verificación es difícil, y no podemos verificar todo el volumen de material que nos va llegando. Por tanto, hemos pensado en formas de lidiar con este problema, como tener un gran grupo de gente con acceso libre a la información y que vaya aportando sus verificaciones según las vaya haciendo. Esto permitiría distribuir y delegar la tarea, y podría funcionar bien.

Pero ¿y si todo el mundo se limitara a publicar de forma anónima y no dispusiéramos de verificadores? ¿Qué pasaría entonces? Para empezar, la estructura sería completamente plana; la información simplemente se enviaría mediante un hash o algo similar. No habría ninguna estructura, solo este documento, ese documento, aquel documento, etcétera. Entonces surgirían personas que desearían influir en el proceso creando mecanismos para esparcir un montón de basura por todas partes, aunque no exista ninguna estructura. ¿Cómo se consigue la información en esta situación? ¿Oyen a sus amigos hablar de ella y luego la comprueban? ¿La vinculan a sus páginas web?

Eric: Se crea una especie de diagrama de influencias.

Julian: Sí, existe un tipo de diagrama de influencias que puedes usar para conseguir información. Puedes inundar Internet con información, pero eso no implica que vayas a inundar el diagrama de influencias con información; eso es algo diferente.

Eric: Pero eso es la historia moderna de los *rankings* y las valoraciones. La web está llena de *spam*, pero el *spam* recibe una valoración baja debido a la influencia, la estructura de los vínculos, etcétera. Está saliendo el sol; tal vez deberíamos intentar terminar el paseo.

EL PROCESO ES EL JUEGO FINAL

Jared: Mientras caminamos, ¿puedo hacerte una última pregunta que tengo en mente desde hace rato? Scott habló antes de la subcultura que se ha desarrollado en torno a todo esto, lo cual es una idea realmente interesante que podemos explorar en el libro, porque plantea la siguiente cuestión: ¿es esta subcultura la que crea la demanda que lleva a la creación de la tecnología, o es la tecnología la que crea la subcultura? Es un debate causa-efecto interesante.

Julian: Bueno, se pueden defender ambas posibilidades, pero en mi opinión es la tecnología la que permite la subcultura. Si cuentas con un montón de gente joven que puede comunicar libremente sus ideas y valores, la cultura surge de forma natural. Esta cultura procede de las experiencias y de la mezcla con otras culturas y cosas por el estilo ya conocidas, pero también procede del temperamento de los jóvenes, de su deseo de encontrar aliados y amigos, de compartir un proceso y de quitar el poder a los mayores.

Lisa: Ja ja ja ja ja.

Scott: Es increíble lo poco creativos que son los mayores.

Eric: En tanto que persona mayor, estoy de acuerdo.

Scott: Yo también hablo como persona mayor.

Eric: En mi opinión, parte de tu argumento consiste en que en el modelo que estás usando, el modelo de Stanford, empiezas con valores humanos y después poco a poco te ves atraído, en mis palabras no en las tuyas, hacia el modelo del estatus; en cierto modo, te van encajonando en la estructura[273]. El sistema de incentivos y restricciones te va metiendo en esa caja a medida que te vas haciendo mayor.

Julian: Exacto. Y con diferentes sistemas que incentivan formas diferentes de transmitir riqueza, de comunicar valores, o de establecer vínculos grupales más eficientes que otros.

Eric: Eso es. Tu argumento es que si te identificas lo suficiente con este nuevo grupo, se producirá un cambio rápido en estos sistemas complejos.

Julian: Precisamente. Sería interesante ver si también se produce algún tipo de cambio de estado. Una revolución es un gran cambio de estado: todo estaba en un estado, y en un momento dado ese todo se precipita en otro estado. Y las transiciones ocurren muy rápidamente. Sería interesante comprobar si vamos a tener un cambio cultural más amplio, general y

globalizado con una transición así de rápida. Es algo que entra dentro de lo posible.

Eric: Sí. Algo que he aprendido es que ahora las cosas ocurren muy rápidamente por la globalización, porque todo está interconectado. Esto antes no era así.

Julian: Información, dinero y riqueza. El principal problema de la globalización es que cualquier capullo puede trasladar su dinero a cualquier parte. Las TEF instantáneas, los movimientos rápidos de riqueza, la firma automática de contratos (que son un tipo de movimiento de riqueza)… todo esto incentiva el oportunismo[274]. Porque si el dinero puede moverse más rápidamente que las sanciones políticas, puedes mover el dinero por todo el sistema, hacer que aumente mientras se mueve y conseguir que se vuelva cada vez más poderoso, y para cuando, fruto del escándalo, se decida detenerlo, ya es demasiado tarde, ya ha desaparecido. Lo que está ocurriendo ahora mismo en Internet es que las sanciones políticas… por cierto, estoy empleando el término «político» en el sentido australiano, que no se refiere a partidos políticos.

Scott: Oh, ¿eso es australiano?

Eric: El estamento político.

Julian: Sí, el estamento político. Ahora las sanciones políticas pueden moverse mucho más rápido que antes, posiblemente tan rápido como el dinero; puede que no a la velocidad de una simple transferencia, pero sí a la de las complejas disposiciones estructurales necesarias para realizar transferencias, que tardan algo más.

Scott: ¿Se te ocurre alguna otra pregunta, Eric? Estás empezando a parecer al teniente Colombo. Julian, has sido muy amable al concedernos tu tiempo.

Jared: Te lo agradecemos mucho.

Lisa: ¿Tienes que llevar un localizador?

Julian: Pues sí, llevo uno en la pierna; una especie de grillete.

Lisa: ¡Un grillete!

Eric: Por curiosidad: dado que, por desgracia, se acerca tu siguiente juicio, ¿tus abogados vienen a verte todos los días?

Julian: Bueno, no pueden venir aquí todos los días desde Londres, porque son ocho horas de viaje entre ida y vuelta. En realidad, acabo de despedir a

algunos de ellos.

Eric: Sí, ya me he enterado. ¿Habláis mucho por teléfono?

Julian: Me estaban cobrando 730 libras la hora por sentarse en un tren para venir desde Londres, incluso después de prometer no hacerlo.

Eric: Entiendo.

Julian: La verdad es que estoy muy descontento con la situación.

Eric: Pero sueles tener visitas todos los días, ¿no? ¿O es algo relativamente inusual?

Julian: Mis empleados y poco más.

Eric: Ah, vale.

Julian: Cada semana suelen venir visitas más interesantes.

Eric: ¡Bueno, espero que al menos te hayamos distraído!

[Risas]

Julian: No nos importaría recibir una filtración de Google, que probablemente sería, creo, sobre lo requerido por la Patriot Act[275].

Eric: Pero eso sería [*susurrando*] ilegal.

[Risas nerviosas]

Julian: ¡Depende de la jurisdicción…!

[Risas entre dientes]

Eric: Pero somos una empresa de…

Julian: Hay leyes más poderosas. La Primera Enmienda, por ejemplo.

Eric: No, en realidad le he dedicado bastante tiempo a esa cuestión, porque tengo algunos problemas por haber planteado una serie de críticas a Patriot I y Patriot II[IX], como por ejemplo que son poco transparentes, que las órdenes judiciales no se publican, etcétera, etcétera. La respuesta es que las leyes estadounidenses son muy específicas respecto a Google. No podríamos hacerlo; sería ilegal.

Julian: Actualmente tenemos una batalla por un caso similar con Twitter. Hemos tenido tres vistas judiciales para intentar conseguir los nombres de las otras compañías que solicitaron las citaciones al gran jurado de Estados Unidos. Twitter se resistió a las citaciones, y precisamente por eso nos enteramos[276]. Argumentaron que se nos debía comunicar que existía una citación; a mí no me lo dijeron, pero sí a otras tres personas.

Scott: ¿Y esto te concernía a ti o a WikiLeaks?

Julian: A mí personalmente, pero sabemos que hay al menos otras cuatro compañías.

Eric: Puedo transmitir tu petición a nuestro consejo de administración.

Julian: Diles que soliciten que se nos comunique.

Eric: Entonces, tu petición concreta es que Google solicite legalmente…

Julian: Sí.

Eric:… que WikiLeaks, en tanto que organización, debería ser informada…

Julian: O a cualquiera de los individuos.

Eric:… o a cualquiera de los individuos, si se les nombra en una FISA[277].

Julian: Sí.

Eric: Muy bien. Lo transmitiré[278].

Julian: Genial.

Eric: ¡Y veremos qué pasa!

Julian: Diles que vengan con todo.

[Risas]

Eric: Luego nos ocuparemos de lo que vamos a hacer a partir de ahora, pero primero dejemos que Julian se ocupe realmente de gestionar el imperio… Hablando de eso —no puedo dejar de hacer preguntas— tengo curiosidad, ¿te dejan seguir gestionando WikiLeaks? Tienes empleados, así que supongo que hablas con ellos

Julian: Sí.

Eric: ¿Les llamas por teléfono? Supongo que puedes usar el correo electrónico, ¿no?

Julian: No, no lo uso.

Eric: ¿Porque está vigilado?

Julian: Es demasiado peligroso. Y el correo electrónico cifrado es casi peor, porque destaca mucho y puede ser blanco de ataques: ¡Es un correo cifrado, atacad, atacad! El problema es que no tenemos teléfonos codificados; por desgracia no funcionan en todos los países, aunque los SMS sí que funcionan.

Eric: Cuando hablas con un miembro de tu personal, ¿normalmente es por teléfono o en persona?

Julian: Normalmente en persona. Ahora tengo que actuar como Osama Bin Laden.

Jared: ¿Cuántos empleados tienes, Julian?

Julian: Unos veinte.

Eric: Entonces, si tuvieras que hacer un resumen aproximado: recibes visitas, utilizas la tecnología con cuidado para gestionar las cosas, y eres consciente de que te vigilan.

Julian: Sí.

Eric: Y por lo que he leído, esto es así desde hace un tiempo.

Julian: Así es desde hace al menos un año y… A comienzos de 2008, uno de nuestros primeros criptógrafos fue abordado por la inteligencia británica en un aparcamiento de Luxemburgo; esa fue la primera…

Eric: ¿Qué hicieron?

Julian: Le siguieron hasta un supermercado, y cuando salió le esperaban en el coche: un hombre de unos cuarenta años, con un buen reloj y buenos zapatos, alto y seguro de sí mismo, con acento británico; un James Bond estereotípico. Empezó a hacerle preguntas sobre WikiLeaks y sobre mí, y le dijo que le gustaría tomar un café y charlar, pero era una clara amenaza: era el aparcamiento de un supermercado; podía haberse acercado en cualquier otro sitio, pero escogió ese aparcamiento.

Lisa: ¿Dijo si era de la inteligencia británica?

Julian: No. Nuestro empleado se marchó, diciendo que no le interesaban los hombres.

[Risas]

Lisa: ¿Cómo saber si eso fue una victoria?

Julian: ¿Cómo lo sabemos o cómo lo sé?

Jared: Lisa ha hecho la mejor pregunta del día.

Eric: ¿Cómo sabéis si habéis ganado?

Julian: Es imposible ganar en este tipo de situaciones; es una lucha continua que la gente ha llevado a cabo durante mucho tiempo. Por supuesto, hay muchas batallas individuales en las que ganamos, pero en general en la naturaleza del ser humano está mentir, engañar y jugar sucio. La gente que no hace nada de esto suele encontrarse y formar grupos organizados, y son más eficientes porque, como tienen esa manera de ser no se mienten, ni se engañan ni juegan sucio el uno con el otro. Es una lucha muy antigua entre oportunistas y colaboradores, y no creo que vaya a terminar nunca. Pienso que podemos hacer avances significativos, y tal vez son precisamente estos avances y la participación en la lucha lo que es bueno para la gente: el proceso es parte del objetivo final. No se trata simplemente de llegar a algún sitio, y de hecho lo más valioso para las personas es el sentimiento de que merece la pena estar involucradas en este proceso y esta lucha.

Scott: Pues es un final satisfactoriamente espiritual.

[Risas]

Lisa: ¿Cómo podemos obtener todo lo grabado para transcribirlo? ¿Cómo lo hacemos?

Julian: Creo que lo más seguro es que os llevéis la cinta.

Lisa: ¿No te importa? ¿La transcribimos y te enviamos todo de vuelta? ¿Lo mandamos por FedEx?

Julian: Sí.

Lisa: ¿Piensas que es… seguro?

[Fin de la grabación]

LÍBRANOS DEL «NO SEAS MALO»

Seguramente los lectores tendrán curiosidad por saber cómo aparecieron finalmente representadas WikiLeaks y las causas que defiende en *The New Digital Age*, para comparar con el material original.

Cuando sale a colación el tema de WikiLeaks —poco menos que un tabú en el entorno del Departamento de Estado de Estados Unidos— Schmidt y Cohen sienten la necesidad de comenzar disculpándose: «Dejando a un lado nuestra… posición», explican, «debemos tener en cuenta lo que los activistas de la libertad de información quieren hacer en el futuro, y por ello Assange es un punto de partida muy útil». Su propia visión es que «una mayor transparencia en todas las cosas para conseguir un mundo más justo, seguro y libre» es «un modelo peligroso»: «los gobiernos han establecido sistemas y normativas muy válidas que, aunque imperfectas, deberían seguir en vigor para tener claro quién toma las decisiones acerca de lo que es información clasificada y lo que no»**[279]**.

Una vez que han tranquilizado convenientemente a su audiencia, se lanzan a ofrecer un resumen educado y altruista. Aluden a mi comentario sobre que la civilización humana está construida a partir de la documentación que tengamos sobre nuestra historia, por lo que tenemos que intentar que esa documentación sea lo más amplia posible, fácilmente consultable y resistente a la censura. Describen uno de los planteamientos teóricos de WikiLeaks: que la publicación de información filtrada solo daña a aquellas organizaciones que están involucradas en acciones que el público no apoya, y que tales organizaciones no pueden evitar producir esta documentación inculpatoria si desean seguir siendo eficientes. Y explican mi preocupación por la censura mediante la complejidad, en la que las operaciones extremadamente complicadas, como las que tienen lugar en los paraísos fiscales, son ostensiblemente abiertas pero totalmente impenetrables.

Hecho el resumen, los autores proceden a servirse de WikiLeaks para establecer claramente su propia posición, apresurándose a llegar a la conclusión de que es «desafortunado» que «personas como Assange y

organizaciones como WikiLeaks estén tan bien situadas para aprovecharse de algunos de los cambios que se van a producir en la próxima década»[280].

¿Por qué piensan que es algo desafortunado? Schmidt y Cohen caen en un argumento utilizado en 2010 por el Pentágono: «La información publicada por WikiLeaks pone vidas en peligro»[281], argumento ampliamente rebatido. En el texto no se proporciona ninguna prueba de ello —y en todo caso las referencias infundadas al riesgo son intelectualmente nulas— aunque incluyen una nota a pie de página. Por desgracia, todo aquel que espere encontrar aunque solo sea la fuente de esta acusación se verá decepcionado. «Como mínimo», dice la nota, «las plataformas como WikiLeaks y los colectivos piratas que trafican con material clasificado robado a los gobiernos permiten o alientan el espionaje»[282].

Por supuesto, el espionaje es algo diferente a poner «vidas en peligro» —una acusación poco precisa reforzada con otra— pero tampoco se ofrece ninguna prueba de que WikiLeaks «permita» el espionaje. Aunque es una incoherencia equiparar la publicación de documentos con la venta privada de secretos de unos estados a otros, eso es precisamente lo que hacen Schmidt y Cohen.

La acusación de espionaje no es un tema baladí: Chelsea Manning está cumpliendo una pena de treinta y cinco años de cárcel tras ser condenada por unos cargos de espionaje bastante creativos. Uno de los objetivos principales de la acusación durante su juicio fue involucrarme en esos mismos cargos de espionaje, criminalizando al mismo tiempo tanto al informante como al editor.

Schmidt y Cohen preguntan a sus lectores: «¿Por qué es Julian Assange, concretamente, quien decide qué información es relevante para el interés público?» y «¿qué ocurre si la persona que toma tales decisiones está dispuesta a aceptar un indiscutible daño a inocentes como consecuencia de sus revelaciones?»[283] Pero estas acusaciones de «daño» de los autores del libro, ni siquiera se corresponden con lo establecido por el gobierno de Estados Unidos. El general de brigada Robert Carr, un oficial estadounidense de contraespionaje, durante el juicio de Manning se vio forzado a admitir bajo juramento que, pese a una búsqueda exhaustiva y presumiblemente desesperada, no pudieron encontrar casos en los que un individuo sufriese daños físicos como consecuencia de las publicaciones de WikiLeaks[284]. Un alto representante de la OTAN en Kabul comunicó a la CNN en octubre de 2010 que no había habido «ni un solo caso en el que los afganos necesitasen protección o traslado debido a la filtración»[285].

Si Schmidt y Cohen consideran que «Julian Assange, concretamente» no debería decidir qué información es relevante para el público, ¿quién debería hacerlo? En la mayoría de las sociedades, estas decisiones son una parte crucial del trabajo de los editores y de los periodistas, supuestamente independientes, del gobierno. Tal vez Schmidt y Cohen creen en el periodismo, pero no en el periodismo realizado «concretamente» por WikiLeaks. Por desgracia, no se trata de eso.

La institución que, en su opinión, debería determinar quién puede publicar es el estado.

Los editores que dan a conocer información confidencial, nos dicen, precisan «supervisión» para que la actividad que realizan sea beneficiosa para la sociedad. En cuanto a quién debería aplicar esta supervisión, sugieren «un organismo central que favorezca la publicación de información»[286], sin ofrecer más detalles ni cuestionarse los evidentes peligros de una visión tan totalitaria.

Schmidt y Cohen, que escribieron esto antes de la aparición de Edward Snowden, especulan que en el futuro las filtraciones serán menos probables, debido a que los gobiernos y las corporaciones empiezan a «ser conscientes de los riesgos que conlleva una ciberseguridad deficiente»[287]. Se preguntan si proliferarán editores incensurables del estilo de WikiLeaks —una «idea irresistible y aterradora»— y concluyen que esto no ocurrirá en Occidente, pero que algunos países en desarrollo experimentarán «su propia versión del fenómeno WikiLeaks» a medida que vayan conectándose a la red global[288].

«Las organizaciones que no puedan atraer filtraciones de alto nivel perderán atención y financiación, y se irán atrofiando de manera lenta pero constante», explican. «Assange desde el punto de vista de su organización, describió esta dinámica como algo positivo. ‘Las fuentes hablan por sus acciones’, dijo; ‘Las fuerzas del mercado nos disciplinan’»[289].

Lo que dije en realidad fue: «El mercado de fuentes nos disciplina», lo que no es más que un error insignificante, pero lo que dicen a continuación sí que es una seria calumnia:

Assange nos dijo que modificaba los textos únicamente para reducir la presión internacional que le estaba ahogando financieramente, y dijo que hubiera preferido no modificarlos[290].

Esto es falso, pero pronto llegó a manos de varias publicaciones, como la revista *Foreign Policy*, a modo de publicidad para el libro de Schmidt y

Cohen, con el práctico título: «El dinero es la única razón por la que Julian Assange modifica los documentos de WikiLeaks»[291].

He aquí el párrafo de la transcripción a que hacen referencia:

Julian Assange: La cuestión es: ¿estas fuentes podrían escoger a otro grupo para publicar su material aunque no disponga de un procedimiento de minimización de riesgos? La respuesta es sí, pero hay que entender la razón principal por la que llevamos a cabo estos procedimientos. No lo hacemos porque la documentación publicada, al revelar información sensible, pueda conllevar un riesgo razonable de producir un daño real fruto de la revelación, ya que eso muy rara vez ocurre. En realidad, lo que sí es bastante probable es que, si no aplicamos este procedimiento, nuestros oponentes intentarán, de manera oportunista, desviar la atención de las revelaciones publicadas —cuestiones muy importantes— insistiendo en la posibilidad de un daño potencial, y por tanto en la posibilidad de que la publicación resulte contraproducente —puesto que lo que queremos es promover la justicia— y de que la organización sea hipócrita. Por ello, muchos de los procedimientos que llevamos a cabo no solo van dirigidos a intentar minimizar el riesgo que puedan correr las personas nombradas en el material, sino que también se trata de minimizar el riesgo de que los oportunistas reduzcan el impacto del material publicado. Así pues, parte del proceso de maximización del impacto que llevamos a cabo es para evitar este tipo de ataques contra lo que publicamos. De este modo, las fuentes comprenderán que lo que hacemos tiene el objetivo de maximizar el impacto. Dicho esto, nosotros no censuramos nunca lo que nos llega. Lo que hacemos es retrasarlo: lo retrasamos hasta que la situación cambie y podemos publicar la información recibida.

Eric Schmidt: Entonces, ¿puede decirse que incluso la documentación censurada acabará siendo publicada tarde o temprano tal y como estaba?

Julian Assange: Sí. […] Me preocupa que no estemos protegiendo nada. Es un terreno muy resbaladizo, y ya he dicho que esto lo hacemos no solo para minimizar daños, sino también por motivos políticos, para impedir que algunas personas intenten desviar la atención de la parte importante de lo publicado centrándose en los posibles riesgos.

La afirmación de que he modificado la información únicamente para reducir la presión financiera internacional sobre WikiLeaks o sobre mí mismo

no tiene la más mínima base.

Schmidt y Cohen se preguntan a continuación: «¿La reacción hubiese sido diferente, sobre todo por parte de los gobiernos occidentales, si WikiLeaks hubiese publicado documentos secretos robados a los gobiernos de Venezuela, Corea del Norte e Irán?». La respuesta es inmediata:

«Teniendo en cuenta la actitud del presidente Obama durante su primer mandato» —claramente con «tolerancia cero» hacia las filtraciones no autorizadas de información secreta sobre altos cargos estadounidenses— «cabría esperar que los próximos gobiernos occidentales acaben adoptando una postura disonante hacia las revelaciones digitales, alentándolas en los países rivales, pero persiguiéndolas ferozmente en el propio»[292].

Los autores ofrecen a continuación una demostración práctica de este tipo de doble rasero. Aunque Schmidt y Cohen afirman que WikiLeaks es «un modelo peligroso» que «pone vidas en peligro» y «permite o alienta el espionaje», se sirven conscientemente de documentos publicados por WikiLeaks para demostrar que China está utilizando proyectos de infraestructura para «extender su influencia en África y en Internet»[293].

Vuelven a tocar el tema de WikiLeaks en un capítulo bastante surrealista llamado «El futuro del terrorismo», concretamente en un apartado subtitulado «El ascenso del terrorismo informático». Sin ofrecer ningún ejemplo histórico de algún «terrorista» informático al que poder agarrarse, vuelven a recaer en «WikiLeaks… y sus simpáticos aliados, los piratas informáticos». Se refieren a las protestas, en forma de denegación de servicio, llevadas a cabo por Anonymous durante la «Operación Vengar a Assange», como respuesta al bloqueo bancario ilegal sobre WikiLeaks. Los autores no lo mencionan, pero las protestas tuvieron lugar mientras yo estuve en prisión sin cargos a finales de 2010. Han pasado tres años y medio, pero actualmente continúa vigente la persecución de los jóvenes supuestamente implicados, los «PayPal 14»[294].

Seguidamente, los autores insinúan que las acciones directas en Internet con motivos políticos entran dentro del espectro del terrorismo. Aunque Schmidt y Cohen admiten que ni WikiLeaks ni Anonymous son grupos terroristas *per se*, escriben: «hay quien afirma que los piratas informáticos que realizan actividades como robar y publicar información personal o secreta no están muy lejos de serlo». La línea de separación entre «los piratas inofensivos y los peligrosos, en la era posterior al 11 de septiembre, es cada vez más difusa», insisten, difuminando aún más dicha línea[295].

Su discurso pasa entonces desde WikiLeaks y Anonymous hacia un terreno más especulativo relacionado con la alarma social, donde queda claro que Schmidt y Cohen viven en otro mundo:

Si bien hoy en día nos enteramos de que los musulmanes de clase media residentes en Europa están viajando a Afganistán para entrenarse como terroristas, puede que en el futuro veamos lo contrario: afganos y pakistaníes que van a Europa para entrenarse como ciberterroristas. A diferencia de los campos de entrenamiento militar, con galerías de tiro y circuitos de obstáculos, los campos de entrenamiento informático podrían ser tan anodinos como unas pocas habitaciones con varios ordenadores portátiles, gestionados por capacitados estudiantes de postgrado descontentos con el sistema en Londres o París. Actualmente los campos militares pueden ser identificados vía satélite, mientras que los campos informáticos resultarían indistinguibles de los cibercafés[296].

LA NUEVA ERA DIGITAL TRAS SNOWDEN

En un «Epílogo para la edición en tapa blanda», publicado tras las primeras revelaciones de Snowden, Schmidt y Cohen retoman la cuestión de las filtraciones, pero en esta ocasión abandonan totalmente la idea de que las filtraciones futuras van a ser cada vez menos probables, pues dicen que «siempre habrá demasiada gente con acceso a demasiada información como para detener las filtraciones masivas […]. En el futuro habrá más Assanges y más Snowdens»[297].

Como buenos occidentales optimistas, los autores afirman que el resultado del debate sobre las revelaciones de Snowden será positivo para Occidente: «Creemos que en última instancia se acabará demostrando que, en los estados occidentales con una historia de protección de los derechos de privacidad, los ciudadanos y los gobernantes irán adquiriendo con el tiempo un equilibrio efectivo entre libertad y seguridad». Aquellos que viven en Estados Unidos son aún más afortunados, ya que «incluso a medida que las herramientas de vigilancia se van volviendo más y más sofisticadas, Estados Unidos, con su experiencia a la hora de mantener el equilibrio entre la garantía de seguridad pública y la preservación de la privacidad […] está bien preparado para recomponer correctamente ese equilibrio». A pesar de todas las pruebas existentes que demuestran que el mayor sistema de vigilancia de la historia de

la humanidad ha sido construido por Estados Unidos, Schmidt y Cohen se resisten a abandonar la clásica clasificación binaria de estados buenos —«donde empresarios y gobernantes operan en el seno de una cultura de responsabilidad, transparencia y libre albedrío»— y estados malos, como China.

¿Y qué hay de la responsabilidad de las propias compañías tecnológicas? Schmidt y Cohen aluden a mi reseña del libro, comentando que no les gusta «la forma en la que las grandes empresas de tecnología pueden amenazar la libertad de los individuos», pero que esto «nos desvía de la verdadera cuestión»[298]. Citan a Edward Snowden por insistir en que las empresas tecnológicas deberían «tener la ‘obligación ética’ de informar de forma más abierta de las peticiones que están recibiendo», pero comentan que tales argumentos «no son buenos». ¿Por qué no? Los autores no especifican, más allá de comentar que «todos nosotros —ciudadanos, empresas y gobierno— [estamos] aún buscando nuestro camino», qué quieren decir cuando hablan de un grado aún mayor de responsabilidad. Los autores prefieren centrarse en la profunda lección que extraen de todo ello para el gobierno estadounidense, que no es otra que «necesita incluir a expertos en informática en la Sala de Situaciones de la Casa Blanca», aunque no mencionan qué gigante de Internet tendría el privilegio de ubicar a sus expertos en torno al presidente.

La realidad es que si en el optimista escenario imaginado por Schmidt y Cohen tiene que producirse una «recomposición» del equilibrio entre libertad y seguridad, esta solo se producirá gracias a la valentía del Sr. Snowden y de sus «cómplices»[299]. En tal caso, resulta extraño que los autores arremetan contra Snowden por no ser «más responsable» en cuanto a «las revelaciones que pueden amenazar la seguridad nacional», y que destaquen la «ironía» de que tuviese que huir a Rusia[300]. No obstante, parecen estar algo confusos, pues al mismo tiempo afirman que se alegran de que «desde entonces, los debates que como país hemos tenido sobre vigilancia han sido mucho más sólidos»[301].

Al leer esto, resulta fácil olvidar que Google recibió dinero de la Asociación Nacional de Seguridad por su papel en el programa PRISM[302]. Si el presidente de Google deseaba que se iniciase un sólido debate de forma «más responsable», cabe preguntarse por qué no lo inició él mismo cuando aquel día del verano de 2011 le pedí que aportase pruebas de lo que estaba ocurriendo. Eso sí que hubiese sido una buena Idea de Google.

TRASFONDO DE «EE. UU. CONTRA WIKILEAKS»

A lo largo de este libro se hacen varias referencias a los acontecimientos recientes de la historia de WikiLeaks y de sus publicaciones, referencias que pueden resultar desconocidas para los lectores poco familiarizados con la actividad de WikiLeaks, por lo que a continuación se ofrece un resumen.

La misión de WikiLeaks consiste en recibir información de informantes anónimos y periodistas censurados, publicar tal información y luego defenderse de los inevitables ataques legales y políticos. De forma rutinaria, los estados y organizaciones poderosas intentan suprimir las publicaciones de WikiLeaks, y en tanto que editor de último recurso, WikiLeaks fue diseñada para soportar este tipo de dificultades.

En 2010, WikiLeaks realizó su serie de publicaciones más conocida hasta la fecha, en la que reveló el abuso sistemático del secretismo oficial en el ejército y el gobierno de Estados Unidos. Estas publicaciones se conocen como *Daño Colateral*, los *Diarios de la Guerra* y el Cablegate, todos ellos aún muy vigentes cuando tuvo lugar la conversación con Eric Schmidt y compañía[303]. La respuesta ha sido un esfuerzo continuo y concertado del gobierno de Estados Unidos y sus aliados para destruir WikiLeaks.

EL GRAN JURADO DE WIKILEAKS

Como consecuencia directa de las publicaciones de WikiLeaks, el gobierno de Estados Unidos inició una investigación criminal, en múltiples frentes, sobre Julian Assange y el personal de WikiLeaks, sus simpatizantes y supuestos asociados.

En Alexandria, Virginia, se creó un gran jurado con el apoyo del Departamento de Justicia y del FBI para que evaluase la posibilidad de presentar cargos contra Julian Assange y otros, incluyendo cargos de

conspiración según la Ley de Espionaje de 1917. En las deliberaciones de un gran jurado no está presente ningún juez ni abogado defensor. Algunos altos cargos estadounidenses han dicho que esta investigación «carece de precedentes en importancia y naturaleza».

Desde entonces, en las sesiones de los comités del Congreso se han escuchado sugerencias de algunos diputados, según las cuales la Ley de Espionaje podría utilizarse como herramienta para arremeter contra los periodistas que «publican conscientemente información filtrada», lo que revela que este enfoque se está normalizando en el sistema de justicia de Estados Unidos[304].

El personal de WikiLeaks y sus asociados fueron sometidos a supervisión encubierta, primero en Alemania y después en Islandia[305]. En septiembre de 2010, en un viaje de Julian Assange desde Estocolmo a Berlín, desaparecieron tres ordenadores portátiles codificados, que habían estado bajo custodia de las autoridades aeroportuarias, y que contenían material periodístico confidencial, incluyendo pruebas de un crimen de guerra. En 2013, WikiLeaks presentó una querella criminal contra las autoridades suecas y alemanas en relación con este incidente[306].

En agosto de 2011, seis agentes del FBI y dos fiscales del Departamento de Defensa de Estados Unidos volaron en un avión privado a Islandia y comenzaron a realizar una serie de interrogatorios encubiertos relacionados con la investigación sobre WikiLeaks, sin informar de ello al gobierno islandés, que al tener conocimiento de estas actividades expulsó a los agentes del país[307]. Al marcharse, se llevaron con ellos a un adolescente islandés —Sigurdur Thordarson, a quien continuaron interrogando en Dinamarca— al que sobornaron para que les entregase unos discos duros suyos que contenían datos robados a WikiLeaks[308]. Una investigación parlamentaria llevada a cabo en 2013 en Islandia reveló que Thordarson se había convertido en el confidente del FBI contra WikiLeaks, y que se le había encargado espiar a Julian Assange y al personal de WikiLeaks como parte de la investigación de Estados Unidos[309].

En 2011, un analista de la fuerza aérea estadounidense destinado en Reino Unido fue objeto de una investigación interna por mostrar signos de apoyo a la misión general de WikiLeaks, y por asistir a las vistas judiciales de Assange en Londres. Los documentos de la investigación, publicados a raíz de una petición de Libertad de Información, especificaban «Comunicación con el enemigo» en el apartado «Alegaciones»[310].

En abril de 2014, el Departamento de Justicia de Estados Unidos presentó un alegato judicial en el que sostenía que la investigación criminal «en múltiples frentes» contra WikiLeaks estaba «en curso» y que debía seguir manteniéndose en secreto[311]. Varias personas se han visto forzadas legalmente a aportar pruebas en las vistas del gran jurado[312]. Los asociados y supuestos asociados de WikiLeaks han sido detenidos en aeropuertos, privados de sus derechos e interrogados por agentes estadounidenses[313]. La documentación judicial correspondiente al juicio de Chelsea Manning, la soldado condenada por filtrar información a WikiLeaks, contiene un archivo del FBI sobre la investigación a WikiLeaks que en aquel momento tenía ya 42 100 páginas, unas 8000 de ellas relacionadas con Manning[314].

LA PERSECUCIÓN A CHELSEA MANNING

Chelsea Manning estuvo detenida sin juicio durante 1103 días, una clara vulneración de su derecho a una justicia rápida. El informador de las Naciones Unidas Juan Méndez descubrió que Manning había sido tratada de forma cruel e inhumana, y que incluso había sido torturada[315]. El gobierno acusó a Manning de ser una de las fuentes periodísticas de WikiLeaks y de treinta y cuatro casos individuales de violación del Código Uniforme de Justicia Militar, incluyendo partes de la Ley de Espionaje, acusaciones cuya condena máxima combinada era de más de cien años de prisión[316].

El tribunal prohibió a Manning alegar en su defensa argumentos como interés público, motivación o ausencia de daño real causado por sus presuntas acciones[317]. Manning ofreció una declaración voluntaria de culpabilidad a cambio de una reducción de condena[318], pero el gobierno le denegó esa posibilidad porque quería condenarla por la totalidad de los cargos. El caso fue a juicio en junio de 2013 con un secretismo sin precedentes, lo que motivó la presentación de sendas querellas por parte de WikiLeaks y del Centro de Derechos Constitucionales. En agosto de 2013, Manning fue hallada culpable de diecisiete de los cargos, y condenada a treinta y cinco años de cárcel[319]. En el momento de publicar este libro, tiene una apelación pendiente de resolución en el Tribunal Militar de Apelaciones Criminales de Estados Unidos[320].

PETICIONES DE ASESINATO PARA JULIAN ASSANGE Y LOS TRABAJADORES CONOCIDOS DE WIKILEAKS

La investigación del gran jurado no es el único ataque que ha sufrido WikiLeaks. En diciembre de 2010, poco después del estallido del Cablegate, varios políticos estadounidense llegaron a solicitar el asesinato extrajudicial de Julian Assange, incluso utilizando para ello vehículos aéreos no tripulados. Algunos senadores tildaron a WikiLeaks de «organización terrorista», y a Assange de «terrorista de alta tecnología» y de «combatiente enemigo» implicado en una «guerra tecnológica»[321].

Un equipo formado por más de 120 miembros del personal del Pentágono se puso al frente de los casos de la publicación de *Diarios de Guerra en Irak* y del Cablegate, dedicándose a «tomar acciones» contra WikiLeaks[322], y también se formaron públicamente grupos de trabajo similares en el FBI, la CIA y el Departamento de Estado de Estados Unidos. El gobierno estadounidense comenzó a presionar a los países aliados para que detuviesen a Julian Assange y prohibiesen a WikiLeaks operar en su territorio[323].

CENSURA DIRECTA

En una serie de actos ilegales de censura, los proveedores de Internet comenzaron a denegar el servicio a wikileaks.org. El 1 de diciembre de 2010, Amazon eliminó a WikiLeaks de su lista de servidores de almacenamiento, y el 2 de ese mismo mes, el servicio de DNS en el dominio wikileaks.org se vio interrumpido. Durante este periodo, WikiLeaks se mantuvo activa gracias a un enorme esfuerzo de reflejo masivo en páginas espejo, por el que miles de simpatizantes se integraron en un sistema de distribución masiva diseñado y coordinado por WikiLeaks, ofreciendo sus servidores para albergar una copia de las publicaciones realizadas en las páginas web, y otros tantos miles distribuyeron las direcciones IP y nombres de dominio alternativos a la página de WikiLeaks a través de las redes sociales[324].

La administración Obama advirtió a los empleados federales que la documentación publicada por WikiLeaks seguía siendo documentación secreta, incluso a pesar de que estaba siendo publicada por algunas de las agencias de noticias más importantes del mundo, como *The New York Times* y

The Guardian. A estos empleados se les dijo que el acceso al material, estuviese en wikileaks.org o en *The New York Times*, sería considerado como una violación de la seguridad. Los organismos gubernamentales como la Biblioteca del Congreso, los departamentos de Comercio y de Educación y el ejército de Estados Unidos, bloquearon el acceso a los contenidos de WikiLeaks a través de sus redes[325]. Esta prohibición no se limitó al sector público, pues los mismos empleados del gobierno también advirtieron a las instituciones académicas que aquellos estudiantes que deseasen hacer carrera como funcionarios públicos deberían evitar el acceso a todo material publicado por WikiLeaks, tanto para sus investigaciones como en su actividad online[326].

Durante el lanzamiento del Cablegate, ocurrido los días 28 y 29 de noviembre de 2010, WikiLeaks tuvo que hacer frente a una «denegación generalizada de servicio» (en inglés, «distributed denial of service», o DDoS)[327]. Este DDoS no consiguió dejar a WikiLeaks fuera de la red, pero sí afectó moderadamente a la disponibilidad de la página durante los ataques.

VIGILANCIA Y CAMPAÑAS DE SUBVERSIÓN CONTRA WIKILEAKS

En 2011 se supo que, a través del bufete de abogados Hunton & Williams LLP, Bank of America había encargado a un grupo de empresas de seguridad que llevase a cabo un análisis interno y ofreciese una respuesta externa a WikiLeaks. Los documentos internos filtrados muestran que una de estas empresas de seguridad, HBGary Federal, propuso la creación de un «Equipo Themis» —un grupo de trabajo privado formado por HBGary Federal, Palantir Technologies, y Berico Technologies— que se encargase de iniciar una campaña de subversión, desinformación y sabotaje contra WikiLeaks, sus asociados e incluso sus simpatizantes, como el periodista Glenn Greenwald[328].

A comienzos de 2014 se publicaron los documentos de la Agencia de Seguridad Nacional obtenidos por Greenwald gracias al informante Edward Snowden, que revelan que el Cuartel General de Comunicaciones del gobierno de Reino Unido (en inglés, GCHQ) había estado vigilando estrechamente a todos y cada uno de los visitantes habituales a la página web de WikiLeaks, registrando sus direcciones IP y sus peticiones de búsqueda en

tiempo real. Estos documentos muestran como el Grupo Conjunto de Inteligencia e Investigación sobre Amenazas (en inglés, el JTRIG) tiene autorización para llevar a cabo «Operaciones encubiertas en Internet», «Operaciones técnicas encubiertas», y «Operaciones basadas en efectos» contra «adversarios» en Internet, incluyendo la infiltración en salas de chat, ataques de «bandera falsa», ataques a redes informáticas, ataques de DDoS; bloqueo de actividades; intervención de teléfonos, ordenadores y cuentas de correo electrónico; y operaciones ofensivas diseñadas para «destruir» y «perturbar» a los adversarios[329]. Estos mismos documentos mostraban los debates internos al más alto nivel entre la oficina del consejo general de la ASN y otros oficiales sobre la posibilidad de declarar a WikiLeaks «actor extranjero malicioso» con el propósito de ponerla en el punto de mira[330].

CENSURA FINANCIERA: EL BLOQUEO BANCARIO

WikiLeaks funciona con las donaciones de sus simpatizantes. En diciembre de 2010, algunas de las instituciones financieras más importantes del mundo, como VISA, MasterCard, PayPal y Bank of America, se plegaron ante la presión extraoficial de Estados Unidos y comenzaron a denegar sus servicios financieros a WikiLeaks, bloqueando todas las transferencias bancarias y donaciones realizadas con los principales tipos de tarjetas de crédito.

Aunque estas instituciones son estadounidenses, su ubicuidad en las finanzas globales implicaba que a los donantes tanto de Estados Unidos como del resto del mundo prácticamente se les cerraba toda posibilidad de entregar dinero a WikiLeaks para apoyar sus actividades de publicación.

El «bloqueo bancario», tal y como se le conoce hoy en día, no forma parte de ningún procedimiento judicial o administrativo[331], pero WikiLeaks sí ha presentado importantes querellas judiciales en diferentes jurisdicciones de todo el mundo para intentar romper el bloqueo. El Tribunal Supremo de Islandia, por ejemplo, falló a favor de WikiLeaks en un juicio contra VISA y Valitor, una de las empresas filiales de MasterCard[332]. Se presentó otra querella ante la Comisión Europea, quien inició una investigación sobre el abuso de posición dominante en el mercado por parte de instituciones involucradas en el bloqueo[333], investigación que aún está abierta en el momento de escribir estas líneas. Como respuesta al bloqueo, el Parlamento

Europeo ha puesto en marcha una legislación dirigida a regular el mercado de servicios financieros[334], y actualmente en Dinamarca está abierto un proceso judicial sobre ello.

A fecha de abril de 2014, el bloqueo había perdido fuerza significativamente gracias al esfuerzo conjunto de WikiLeaks y de sus aliados. WikiLeaks se las ha arreglado para crear formas de donación mediante portales apoderados de pago, que por el momento no han sido clausurados[335]. Además, algunos de los protagonistas del bloqueo han llevado a cabo una retirada silenciosa parcial o total, abriendo una vía de indemnización[336].

INCAUTACIÓN DE REGISTROS ELECTRÓNICOS

El 14 de diciembre de 2010, Twitter recibió una «citación administrativa» del Departamento de Justicia de Estados Unidos en la que se le ordenaba entregar toda la información disponible que pudiese ser relevante para una investigación sobre WikiLeaks, citación que llegó con el nombre de Orden 2703(d), en referencia a una sección de la Ley de Almacenaje de Información («Stored Communications Act»). Amparándose en esta ley, el gobierno de Estados Unidos reclamaba para sí la autoridad para forzar la revelación de archivos electrónicos de comunicación privadas sin necesidad de una orden judicial de registro, lo que, en la práctica, le permitía esquivar las protecciones contra registros e incautaciones arbitrarias establecidas por la Cuarta Enmienda de la Constitución.

La citación exigía la entrega de nombres de usuarios, archivos de correspondencia, direcciones, números de teléfono, detalles de cuentas bancarias y números de tarjetas de crédito de cuentas y personas asociadas a WikiLeaks, incluyendo Julian Assange, el experto en investigación y *software* Jacob Appelbaum, la parlamentaria islandesa Birgitta Jónsdóttir, el empresario holandés Rop Gonggrijp, Chelsea Manning y la propia WikiLeaks. Según los términos de la citación, Twitter ni siquiera podía revelar a todas estas personas la existencia de esta orden, pero Twitter recurrió con éxito contra esta prohibición y obtuvo el derecho a informar a los interesados de la orden que requería sus archivos.

Poco después de publicarse la noticia de la citación, WikiLeaks realizó un llamamiento público a Google y Facebook, instándoles a revelar cualquier otra citación gubernamental relacionada con el caso[337]. Ninguna de las dos compañías se dignó a responder.

Al conocer la existencia de la citación de Twitter, el 26 de enero de 2011 Appelbaum, Jónsdóttir, y Gonggrijp —representados por Keker & Van Nest, la Unión Estadounidense de Libertades Civiles y la Electronic Frontier Foundation— pidieron a sus abogados que presentasen una moción conjunta para invalidar la orden, moción que ha dado en llamarse el «caso de la citación de Twitter»[338]. El abogado de Appelbaum presentó posteriormente otra moción en la que solicitaba la publicación de los documentos judiciales secretos sobre los intentos del gobierno para obtener sus datos privados en Twitter o en otras compañías. Ambas mociones fueron denegadas por un magistrado estadounidense el 11 de marzo de 2011. Los demandantes presentaron un recurso de apelación.

El 23 de junio de 2011, durante la conversación transcrita en este libro, Julian Assange solicitó personalmente al presidente de Google, Eric Schmidt, que informase a WikiLeaks de cualquier orden gubernamental secreta de petición de información relacionada con WikiLeaks o sus asociados. Schmidt se negó, alegando que las peticiones de datos por parte del gobierno incluían cláusulas de confidencialidad, pero dijo que informaría de la petición al departamento legal de Google. Desde entonces, Google no ha realizado comunicación alguna relativa a las peticiones de datos realizadas por el gobierno.

El 9 de octubre de 2011, *The Wall Street Journal* reveló que el servidor de correo electrónico Sonic.net, con base en California, también había recibido una citación exigiéndole los datos de Jacob Appelbaum. Sonic litigó contra la orden del gobierno y perdió, pero obtuvo permiso para informar al interesado de que estaba obligado a entregar sus datos. El mismo periódico informó también de que Google había recibido una citación similar, pero no aclaró si Google había luchado judicialmente contra ella[339].

El 10 de noviembre de 2011, un juez federal falló en contra de Appelbaum, Jónsdóttir y Gonggrijp, y ordenó que Twitter entregara sus datos al Departamento de Justicia[340]. El 20 de enero de 2012, los demandantes volvieron a recurrir, solicitando la anulación de la negativa a revelar la posible existencia de órdenes enviadas a otras compañías distintas de Twitter[341]. El 23 de enero de 2013, el Tribunal de Apelación de Estados Unidos denegó nuevamente la petición de los demandantes, al considerar que

la revelación de otras órdenes comprometería la investigación criminal del gobierno[342]. Ya no hubo más recursos.

El 7 de junio de 2013, los documentos publicados por Edward Snowden revelaron la existencia de PRISM, un programa secreto que otorgaba a la ASN acceso a los servidores privados de un grupo de grandes compañías de servicios electrónicos, incluyendo Microsoft, Skype, Facebook, Apple y Google[343].

El 18 de junio de 2013, dos exvoluntarios islandeses de WikiLeaks, Herbert Snorrason y Smári McCarthy, recibieron sendos correos electrónicos de Google que incluían órdenes judiciales de registro, hasta el momento secretas, que le permitían incautarse de la totalidad del contenido de sus cuentas de Gmail. Las órdenes databan del verano de 2011, pero Google había esperado hasta la expiración de sus cláusulas de confidencialidad, en 2013, para informar a los dos hombres de su existencia[344]. Google no ha revelado la existencia de otras órdenes similares relacionadas con el personal o los asociados de WikiLeaks, pero la aparición de órdenes dirigidas contra personas periféricas a la organización como Snorrason y McCarthy indica que es muy probable que tales órdenes existan y permanezcan en secreto.

AMENAZAS CONCURRENTES

Además de la investigación del gran jurado sobre la publicación de documentos en 2010, las autoridades estadounidenses iniciaron otra investigación simultánea sobre otra publicación de documentos realizada en 2012 por la compañía privada de inteligencia Stratfor.

Los gobiernos de Estados Unidos y de Reino Unido han puesto en marcha además un proceso criminal por la publicación de documentos secretos de la ASN y el GCHQ por parte del informante Edward Snowden. Y la editora de investigaciones de WikiLeaks, Sarah Harrison, ciudadana británica que ayudó a Snowden a eludir su captura huyendo de Hong Kong, ha sido advertida de que no regrese a su país porque corre el riesgo de ser acusada de cómplice[345].

ASILO

En junio de 2012, temiendo la persecución del gobierno estadounidense, Julian Assange entró en la embajada de Ecuador en Londres y solicitó formalmente asilo político[346].

Tras dos meses de deliberaciones, durante los que el gobierno británico amenazó con entrar por la fuerza en la embajada, lo que hubiese supuesto una violación de la Convención de Viena, el gobierno ecuatoriano consideró que el acoso de Estados Unidos a Julian Assange y a WikiLeaks constituía una persecución según los términos de la ley internacional[347], y el asilo fue concedido[348].

En el momento de la publicación de este libro, Julian Assange lleva dos años recluido en la embajada ecuatoriana en Londres, de donde no puede salir porque el gobierno de Reino Unido le amenaza con detenerle si lo hace.

AGRADECIMIENTOS

Con todo mi cariño doy las gracias al equipo de WikiLeaks: Sarah, Joseph, Kristinn y todos los demás —igualmente irreemplazables— que no puedo nombrar aquí; a nuestros amigos seguidores, que nos mantienen con vida; a nuestros aliados, que ya saben quiénes son; a nuestros abogados, que son muchos y todos ellos muy apreciados; a Eric, Jared, Lisa y Scott, por animarme a sentarme a escribir; a Ecuador y su gente, que se han portado muy bien conmigo, y sin cuya protección no podría haber escrito este libro; a E. I. y B. H., que han pasado muchas noches en vela para hacerlo posible; a todo el personal de OR Books, especialmente, Colin, John y Alex, por su paciencia y apoyo; y a todos los que luchan por la libertad: Chelsea Manning, Jeremy Hammond, Barrett Brown, Rudolf Elmer, Gottfrid Svartholm Warg, Peter Sunde Kolmisoppi, John Kiriakou, Edward Snowden, PayPal 14, y a todas las personas anónimas de gran coraje y conciencia que continúan inspirando al resto del mundo.

NOTAS SOBRE LAS REFERENCIAS

Para evitar la «rotura» de los enlaces propuestos, la mayoría de las páginas web citadas en este libro se han referido a través del servicio de almacenaje **archive.today**

Pinche en el enlace de **archive.today** de las notas a pie de página para acceder a la referencia en la página original.

En caso de que **archive.today** no esté disponible, existe una copia de cada enlace en **when.google.met.wikileaks.org**

Para acceder a dichas copias, simplemente sustituya en el enlace **archive.today** por **when.google.met.wikileaks.org**

Por ejemplo, para el enlace **archive.today/r2rur**, teclee **when.google.met.wikileaks.org/r2rur**

Todas las referencias están incluidas en un archivo en el siguiente enlace magnético:

magnet:?xt=urn:btih:744ac8007e1e72e99fc27c561916b3b48daef743



Julian Assange, periodista y programador australiano, es el creador y director de la red Wikileaks, la organización sin fines de lucro que desde hace años publica documentos de interés público, provocando enojo en gobiernos y asombro en la ciudadanía.

Nació el 3 de julio de 1971 en Queensland, Australia, y desde su adolescencia se interesó por la programación. En 1991 Assange fue detenido en Melbourne por *hackear* computadoras de una universidad australiana y de otras instituciones y se declaró culpable de 24 delitos informáticos. Fue detenido, pero liberado al poco tiempo por buena conducta y tras pagar una multa. Aunque gran parte de sus conocimientos se deben a que es autodidacta, estudió en varios colegios secundarios y en otras tantas universidades, donde se especializó en matemática, física, neurociencia y filosofía. La revista Time lo eligió “Hombre del Año” y fue premiado en varias oportunidades por su defensa al derecho de información, pero no todos son reconocimientos para Assange. Varios colaboradores del sitio Wikileaks se refirieron a él como un hombre autoritario, paranoico y que “armó sobre él mismo una imagen de James Bond”. El ex-portavoz de Wikileaks, el alemán Daniel Domscheit-Berg, se alejó de la organización por diferencias con Assange y meses después publicó el libro “Dentro de WikiLeaks”, en el que revela que las cosas fueron cambiando en la red con el correr de los años.

Notas

[1] En 2011 la compañía estaba valorada en 200 000 millones de dólares y daba empleo a 33 077 personas, mientras que actualmente su valor se ha duplicado (400 000 millones de dólares) y sus empleados han aumentado hasta los 49 829. Ver «Investor Relations: 2012 Financial Tables», Google, archive.today/Iux4M. Para el primer trimestre de 2014, ver también «Investor Relations: 2014 Financial Tables», Google, archive.today/35IeZ <<

[2] Para un análisis pormenorizado del libro de Schmidt y Cohen que trata además otros temas similares y que facilitó parte de la investigación para este libro, ver Joseph L. Flatley, «Being cynical: Julian Assange, Eric Schmidt, and the year’s weirdest book», *Verge*, 7 de junio de 2013, archive.today/gfLEr <<

[3] El perfil de Jared Cohen puede verse en la web: archive.today/pkgQN <<

[4] Shawn Donnan, «Think again», *Financial Times*, 8 de julio de 2011, archive.today/ndbmj. Ver también Rick Schmitt, «Diplomacy 2.0», *Stanford Alumni*, mayo/junio 2011, archive.today/Kidpc <<

[5] Eric Schmidt y Jared Cohen, «The Digital Disruption: Connectivity and the Diffusion of Power», *Foreign Affairs*, noviembre/diciembre 2010, archive.today/R13l2 <<

[6] «Alianza de los conectados» (en inglés, *Coalition of the connected*), es un término aparentemente diseñado para asemejarse a «Alianza de la voluntad» (*Coalition of the willing*), utilizado para denominar a la alianza de países liderada por Estados Unidos que durante los meses previos a la invasión de Irak de 2003 funcionó sin la aprobación del Consejo de Seguridad de la ONU. <<

[7] El término «deber de protección», también llamado «responsabilidad de protección», o «R2P» (*Responsibility to protect*) es una «norma emergente» altamente controvertida en el derecho internacional. La R2P se sirve del discurso de derechos humanos para imponer «intervenciones humanitarias» por parte de «la comunidad internacional» en aquellos países cuya población se considera en peligro. En opinión del sector liberal estadounidense que rehúye el imperialismo puro y duro de Paul Wolfowitz (ver Patrick E. Tyler, «U.S. strategy plan calls for insuring no rivals develop», *The New York Times*, 8 de marzo 1992, archive.today/Rin1g), R2P no es más que la justificación en la que se escudan los occidentales para realizar intervenciones militares en Oriente Medio y otros lugares, como lo prueba su ubicuidad en los intentos de invasión de Libia en 2011 y de Siria en 2013. La antigua jefa de Jared Cohen en el Departamento de Estado, Anne-Marie Slaughter, se refirió a ello como «el cambio más importante en nuestro concepto de soberanía desde el Tratado de Westfalia en 1648». Ver su alabanza del libro *Responsibility to Protect: The Global Moral Compact for the 21st Century*, editado por Richard H. Cooper y Juliette Voïnov Kohler, en la página web de la editorial Palgrave Macmillan, archive.today/0dmMq

Para un ensayo crítico sobre la R2P, ver el discurso de Noam Chomsky sobre esta doctrina ante el pleno de las Naciones Unidas: «Statement by Professor Noam Chomsky to the United Nations General Assembly Thematic Dialogue on Responsibility to Protect», Naciones Unidas, Nueva York, 23 de julio de 2009, is.gd/bLx3uU. También disponible en **http://www.un.org/ga/president/63/interactive/protect/noam.pdf**

Ver también «Responsibility to protect: An idea whose time has come — and gone?», *The Economist*, 23 de julio de 2009, archive.today/K2WZJ **<<**

[8] Bridget Johnson, «Biden: Mubarak not a dictator, protests not like Eastern Europe», *The Hill*, 28 de enero de 2011, archive.today/L7EcI <<

[9] Ibid. <<

[10] Chris McGreal, «Tony Blair: Mubarak is ‘immensely courageous and a force for good’», *The Guardian*, 2 de febrero de 2011, archive.today/SIsmb <<

[11] «Secretary Clinton in 2009: ‘I really consider President and Mrs. Mubarak to be friends of my family’», *ABC News*, 31 de enero de 2011, archive.today/8NAoz <<

[12] Richard Smallteacher, «Egypt–Egypt–U.S. intelligence collaboration with Omar Suleiman ‘most successful’», WikiLeaks, 1 de febrero de 2011, archive.today/neBhy <<

[13] Ver «Secretary of State Hillary Clinton’s Speech on Internet Freedom *updated*», *Secretary Clinton Blog*, 15 de febrero de 2011, archive.today/nChdl

Los propios activistas egipcios estaban bastante confundidos. En abril de 2011, el activista Basem Fathy comunicó a *The New York Times* que «aunque apreciábamos la instrucción recibida por las ONG patrocinadas por Estados Unidos, que sin duda nos ayudó en nuestra lucha, éramos igualmente conscientes de que el mismo gobierno también estaba instruyendo al servicio estatal de investigación, responsable del acoso y el encarcelamiento de muchos de nosotros». Ron Nixon, «U.S. Groups Helped Nurture Arab Uprisings», *The New York Times*, 14 de abril de 2011, archive.today/bJyGP <<

[14] «Clinton on a WikiLeaks ‘apology tour’», UPI, 10 de enero de 2011, archive.today/AYRCx <<

[15] El bloguero tunecino Sami Ben Gharbia, miembro de Naawat, lo expresó de la siguiente manera: «Pasaron veinte días entre la publicación de los comunicados de Tunileaks, realizada el 28 de noviembre de 2010, y el comienzo de la Primavera Árabe, el 17 de diciembre de 2010. Ese fue el día en el que un pobre vendedor callejero llamado Mohamed Bouazizi se prendió fuego en plena calle. En una conversación mantenida con un periodista británico ese mismo año, el ministro de propaganda de Ben Ali Oussama Romdhani confesó que "Tunileaks fue el golpe de gracia, aquello que acabo definitivamente con el sistema de Ben Ali" El detonante no fue la información sobre la corrupción y el amiguismo; los tunecinos no necesitaban que WikiLeaks les dijese que su país estaba totalmente corrompido, y de hecho la corrupción había sido objeto de chismorreos y chistes durante años. Lo que realmente marcó la diferencia fue el efecto psicológico de un sistema político enfrentado repentinamente y de forma tan pública a su propia imagen, fea y descompuesta; ahora el gobierno sabía fehacientemente que todo el mundo, tanto dentro como fuera del país, era consciente de lo corrupto y autoritario que era. Y lo mejor era que el que hacía la revelación no era un disidente ni un conspirador político, sino el mismísimo Departamento de Estado de Estados Unidos, un supuesto aliado». Sami Ben Gharbia, «Chelsea Manning and the Arab Spring», *Nawaat*, 28 de febrero de 2014, archive.today/pw0p9

Otro artículo escrito por Sami Ben Gharbia, publicado apenas unos meses antes del comienzo de la Primavera Árabe, hace hincapié en el tema de la agenda estadounidense relativa a la «libertad de Internet» en Oriente Medio y el norte de África. Sami Ben Gharbia, «The Internet Freedom Fallacy and the Arab Digital Activism», *Nawaat*, 17 de septiembre de 2010, archive.today/aoTrj <<

[16] «Clinton on a WikiLeaks ‘apology tour’», UPI, 10 de enero de 2011, archive.today/AYRCx <<

[17] Brian Whitaker, «Gaddafi versus Kleenex», 18 de enero de 2011, disponible en al-bab.com en «Libya: The fall of Colonel Gaddafi», archive.today/lxF1u

Jillian C. York, «Qaddafi's View of the Internet in Tunisia», jilliancyork.com, 16 de enero de 2011, archive.today/GFRQC <<

[18] Greg Grandin, «With Ollanta Humala's Win, Peru Joins Latin America's Left Turn», *The Nation*, 7 de junio de 2011, archive.today/8cvxx

Ver también Nikolas Kozloff, «WikiLeaks cables: The great equaliser in Peru», *Al Jazeera*, 2 de junio de 2011, archive.today/wBacn <<

[19] Durante un recital ofrecido a los participantes de las protestas de Wisconsin, el guitarrista y compositor Tom Morello (Rage Against the Machine, Audioslave, Nightwatchman, Street Sweeper Social Club, «Multi-Viral» por Calle 13 con Tom Morello, Julian Assange y Kamilya Jubran), leyó en voz alta una carta de solidaridad que le había enviado Moar Eletrebi, uno de los organizadores de las protestas de la plaza Tahrir, que decía lo siguiente: «A nuestros amigos de Madison, Wisconsin: nos gustaría que pudieseis conocer de primera mano los cambios que hemos logrado provocar aquí. La justicia es hermosa, pero nunca es gratuita. La belleza de la plaza Tahrir puede trasladarse a todas partes, a cualquier esquina de vuestra ciudad o a vuestros corazones. Por tanto, ¡respirad hondo y manteneos firmes sin desfallecer, pueblo de Wisconsin! Nuestra fortuna está en la brisa, tanto en Oriente como en Occidente. Respirad hondo, Wisconsin, porque la justicia está en el aire, y ojalá que el espíritu de la plaza Tahrir se encuentre en cada uno de los corazones que palpitan hoy en las calles de Madison». Tom Morello, «Frostbite and Freedom: Tom Morello on the Battle of Madison», *Rolling Stone*, 25 de febrero de 2011, archive.today/nTB6h <<

[20] Manning pasó buena parte del primer año de su periodo de detención sin juicio recluida en solitario en un calabozo de los marines estadounidenses en Quantico, Virginia, bajo unas condiciones que el Informador Especial de la ONU Juan Méndez describió como «crueles, inhumanas y degrandantes», bordeando incluso la tortura. La defensa de Manning sugirió que este tratamiento se había aplicado con el fin de forzarla a realizar una «confesión» que implicase a WikiLeaks. El presidente Barack Obama afirmó que las condiciones de Manning eran «apropiadas y conforme a nuestros estándares básicos», pero hasta trescientos especialistas en Derecho, entre ellos el catedrático de Harvard Laurence Tribe, antiguo profesor del propio Obama, denunciaron públicamente el abuso. Por su parte, el portavoz del Departamento de Estado Philip J. Crowley dijo que el trato de Manning por parte del Pentágono era «ridículo, contraproducente y estúpido», y poco después presentó su dimisión. Una campaña internacional logró ejercer una gran presión diplomática sobre el gobierno estadounidense, de forma que Manning fue trasladada a Fort Leavenworth, Kansas, y el mencionado centro de reclusión de Quantico, Virginia, fue clausurado de forma permanente.

Para más detalles acerca del inhumano trato a Chelsea Manning, ver «Trasfondo de EE. UU. contra WikiLeaks». <<

[21] Esto se conoce como el escándalo federal de HBGary. Para más detalles, ver «Trasfondo de EE. UU. contra WikiLeaks». <<

[22] Barrett Brown es un periodista freelance cuya investigación sobre la industria de la seguridad hizo que las autoridades estadounidenses cayesen pesadamente sobre su cabeza. Brown fue detenido en septiembre de 2012 y se le denegó el derecho a la libertad bajo fianza; en octubre de ese año fue acusado de tres cargos relacionados con supuestas amenazas realizadas contra un agente del FBI, y en diciembre se le acusó de doce cargos más relativos a su trabajo como periodista sobre un supuesto delito de pirateo informático en la empresa de inteligencia Stratfor, radicada en Texas, ocurrido el año anterior. Ver Glenn Greenwald, «The persecution of Barrett Brown—and how to fight it», *The Guardian*, 21 de marzo de 2013, archive.today/tUnJ9

Ver también Douglas Lucas, «Barrett Brown's new book 'Keep Rootin' for Putin' skewers mainstream media pundits», *Vice*, 25 de febrero de 2014, archive.today/oS5qv

Ver también Christian Stork, «The Saga Of Barrett Brown: Inside Anonymous and the War on Secrecy», *WhoWhatWhy*, 21 de febrero de 2013, archive.today/mUtJE

La sentencia máxima posible, dados los cargos presentados contra Brown, era de 105 años. Ver Kristin Bergman, «Adding up to 105: The Charges Against Barrett Brown», Digital Media Law Project, 6 de agosto de 2013, archive.today/TQrdR

Uno de los cargos que alegaba amenazas contra un agente del FBI estaba basado en un mensaje publicado por Brown en su cuenta de Twitter que decía: «Los muertos no pueden filtrar información […] disparar ilegalmente al hijo de perra». Lo cierto es que esto no era una amenaza a ningún agente del FBI, sino que Brown se había limitado a citar una petición explícita para que me asesinaran, realizada por el comentarista de la Fox Bob Beckel el 6 de diciembre de 2010 en directo en esta cadena. Mientras que Brown fue acusado de citar las palabras de Beckel para criticarlas, el propio Beckel no fue acusado de cargo alguno. Ver «Fox News' Bob Beckel Calls For 'Illegally' Killing Assange: 'A Dead Man Can't Leak Stuff' (vídeo)», *The Huffington Post*, 7 de diciembre de 2010, archive.today/XiUNo

A comienzos de 2014 Brown negoció un acuerdo sobre su declaración de culpabilidad, y en el momento de escribir estas líneas se espera la sentencia

para finales de dicho año. A finales de abril de 2014, Brown llevaba ya detenido sin juicio un año, siete meses y dieciocho días. Ver «Barrett Brown Signs Plea Deal», página web Free Barrett Brown, 3 de abril de 2014, archive.today/SNMda

En septiembre de 2003, WikiLeaks publicó una declaración sobre la persecución contra Barrett Brown. «Editorial: Release Barrett Brown», WikiLeaks, 16 de septiembre de 2013, archive.today/lROIX <<

[23] El 5 de diciembre de 2010, poco después de que VISA, MasterCard, PayPal, Amazon y otras compañías financieras comenzasen a denegar la prestación de servicios a WikiLeaks, emergió un debate en el foro oficial online sobre el riesgo de realizar donaciones a WikiLeaks mediante Bitcoins, pues ello podía atraer una atención no deseada del gobierno sobre la entonces naciente criptodivisa. «En mi opinión, hay que ir a por todas», escribió un participante. «Satoshi Nakamoto» (seudónimo), el inventor del Bitcoin, respondió: «No, no vamos a 'ir a por todas'. El proyecto necesita crecer de forma gradual para que el *software* pueda ir ganando la fuerza necesaria al ritmo adecuado. Desde aquí hago un llamamiento a WikiLeaks para que se abstenga de utilizar el Bitcoin, pues es un sistema aún en fase experimental y con mucho camino por delante hasta que resulte realmente útil. Por ahora no se podría obtener más que calderilla, y el calor generado por su uso descontrolado en esta fase tan temprana nos destruiría». Ver el Foro sobre el Bitcoin: archive.today/Gvonb#msg26999

Seis días después, el 12 de diciembre de 2010, el famoso Satoshi abandonó la comunidad del Bitcoin, pero antes publicó este mensaje: «Hubiera preferido recibir toda esta atención en cualquier otro contexto. WikiLeaks ha destruido prematuramente el nido de avispas, y el enjambre se dirige furioso directamente hacia nosotros». Ver el Foro sobre el Bitcoin: archive.today/XuHCD#selection-1803.0-1802.1

WikiLeaks leyó el análisis de Satoshi y se mostró de acuerdo con él, por lo que tomó la decisión de aplazar el lanzamiento del canal de donaciones en Bitcoins hasta que la divisa se hubiese estabilizado. Pasado el momento de presión, WikiLeaks hizo pública finalmente su dirección para donaciones en Bitcoins el 14 de junio de 2011. Ver el anuncio en el Twitter de WikiLeaks: archive.today/1hscT

Ver también el Explorador de Bloques de Bitcoin para encontrar la dirección de donación pública de WikiLeaks: is.gd/wJp3tX <<

[24] Para más detalles, ver «Extraditing Assange» en la página web Justice for Assange: archive.today/6izpC <<

[25] Ver por ejemplo la declaración de diciembre de 2010 del entonces fiscal general australiano, el general Robert McClelland, sobre WikiLeaks: «Doorstop on leaking of US classified documents by WikiLeaks», página web del fiscal general del Estado de Australia, 29 de noviembre de 2010, archive.today/Qirks

El término «totalidad del gobierno» aún estaba en uso en marzo de 2012, como lo prueba el informe «Puntos a tratar por la totalidad del gobierno relativos a WikiLeaks» recibido desde el despacho del fiscal general amparándose en el derecho de Libertad de Información: is.gd/MzxG58

Los comunicados diplomáticos obtenidos bajo este derecho, procedentes del Departamento de Asuntos Exteriores y Comercio de Australia, también revelaban la celebración de reuniones privadas con funcionarios estadounidenses relativas a la investigación sobre WikiLeaks «sin precedentes tanto en escala como en naturaleza», archive.today/OAdui <<

[26] Philip Shenon, «The General Gunning for WikiLeaks», *Daily Beast*, 12 de septiembre de 2010, archive.today/Onf0m <<

[27] «DOJ Continues Its ‘Multi-Subject’ Investigation of WikiLeaks», *emptywheel*, 26 de abril de 2014, archive.today/g7zwa

Ver también Philip Dorling, «Assange targeted by FBI probe, US court documents reveal», *Sydney Morning Herald*, 20 de mayo de 2014, archive.today/zFhv7

Para examinar los documentos legales mencionados en el artículo del *Sydney Morning Herald*, ver Case 1:12-cv-00127-BJR en el Tribunal de Distritos de Estados Unidos para el Distrito de Columbia: is.gd/hvvmgM

Para más información acerca del gran jurado, ver «Trasfondo de EE. UU. contra WikiLeaks» <<

[28] «Cablegate», WikiLeaks: **http://www.wikileaks.org/cablegate**

«Gitmo Files», WikiLeaks: **http://www.wikileaks.org/gitmo** <<

[29] El Grupo de Crisis Internacionales se considera a sí mismo como una «organización independiente no gubernamental sin ánimo de lucro» que trabaja «con base en análisis sobre el terreno y con un alto nivel de compromiso a la hora de prevenir y resolver conflictos potencialmente mortales». Por otro lado, también ha sido descrito como «un grupo de expertos de alto nivel […] [concebido] principalmente para proporcionar asesoramiento político a los gobiernos implicados en la remodelación de los Balcanes liderada por la OTAN». Ver Michael Barker, «Imperial Crusaders For Global Governance», *Swans Commentary*, 20 de abril de 2009, archive.today/b8G3o

El perfil de Malcomson como miembro del Grupo de Crisis Internacionales está disponible en fromcrisisgroup.org, archive.today/ETYXp <<

[30] Se podría afirmar que esto es la prueba viviente de la débil hipótesis de Sapir-Whorf. Ver «Linguistic Relativity», Wikipedia, archive.today/QXJPx <<

[31] Glenn Greenwald, «Fact and myths in the WikiLeaks/The Guardian saga», *Salon*, 2 de septiembre de 2011, archive.today/5KLJH

Ver también Matt Giuca, «WikiLeaks password leak FAQ», *Unspecified Behaviour*, 3 de septiembre de 2011, archive.today/ylPUp

Ver también «WikiLeaks: Why The Guardian is wrong and shouldn't have published the password», *Matt's Tumblr*, 1 de septiembre de 2011, archive.today/aWjj4 <<

[32] Andrew Jacobs, «Visit by Google Chairman May Benefit North Korea», *The New York Times*, 10 de enero de 2013, archive.today/bXrQ2 **<<**

[33] Tiempo después, Jeremy Hammond, un joven y valiente revolucionario digital de elevados principios, sería acusado por el gobierno estadounidense de escamotear estos documentos y entregárselos a WikiLeaks. Actualmente es un prisionero político en Estados Unidos, sentenciado a diez años de cárcel tras hablar con un informador del FBI. <<

[34] Yazan al-Saadi, «StratforLeaks: Google Ideas Director Involved in ‘Regime Change’», *Al Akhbar*, 14 de marzo de 2012, archive.today/gHMzq <<

[35] «Re: GOOGLE & Iran ** internal use only — pls do not forward **», correo electrónico ID 1121800 (27 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/sjxuG <<

Para más comentarios internos de Stratfor sobre Jared Cohen y Google, ver:

«Egypt - Google ** Suggest you read», correo electrónico ID 1122191 (9 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/DCzlA

«Re: More on Cohen», correo electrónico ID 1629270 (9 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/opQ3a

«Re: Google Shitstorm Moving to Gaza (internal use only)», correo electrónico ID 1111729 (10 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/vpK3F

«Re: Google's Cohen Activist Role», correo electrónico ID 1123044 (10 de febrero de 2011), Global Intelligence Files, WikiLeaks, 11 de marzo de 2013, archive.today/nvFP6

«Re: movements.org founder Cohen», correo electrónico ID 1113596 (11 de febrero de 2011), Global Intelligence Files, WikiLeaks, 6 de marzo de 2012, archive.today/ToYjC

«Re: discussion: who is next?», correo electrónico ID 1113965 (11 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/ofBMr

«GOOGLE Loose Canon Bound for Turkey & UAE (SENSITIVE - DO NOT FORWARD)», correo electrónico ID 1164190 (10 de marzo de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/Jpy4F

«Re: [alpha] GOOGLE - Cohen & Hosting of Terrorists», correo electrónico ID 1133861 (22 de marzo de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/OCR78

«[alpha] Jared Cohen (GOOGLE)», correo electrónico ID 1160182 (30 de marzo de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/FYQYe

Para estos correo electrónicos y otros, ver el listado de fuentes en: when.google.met.wikileaks.org

[36] «Re: GOOGLE’s Jared Cohen update», correo electrónico ID 398679 (14 de febrero de 2011), Global Intelligence Files, WikiLeaks, 14 de marzo de 2012, archive.today/IoFw4

Este correo electrónico está incluido en el listado de fuentes en: when.google.met.wikileaks.org <<

[37] «Using connection technologies to promote US strategic interests in Afghanistan: mobile banking, telecommunications insurance, and co-location of cell phone towers», identificación canónica: 09KABUL2020_a, Public Library of US Diplomacy, WikiLeaks, archive.today/loAlC

Este comunicado está incluido en el listado de fuentes en:

when.google.met.wikileaks.org

En mayo de 2014, WikiLeaks reveló que la Agencia de Seguridad Nacional (ASN) había obtenido el acceso a todas las llamadas de teléfonos móviles afganos y las estaba grabando todas para una posible recuperación y escucha posterior. Ver «WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA», WikiLeaks, 23 de mayo de 2014, archive.today/lp6Pl <<

[38] De la Biblioteca Pública de Diplomacia Estadounidense, WikiLeaks, ver comunicados con la identificación canónica: 07BEIRUT1944_a, 08BEIRUT910_a, 08BEIRUT912_a, 08BEIRUT918_a, 08BEIRUT919_a, 08BEIRUT1389_a, y 09BEIRUT234_a. Listado disponible en: archive.today/34MyI

Ver también el listado de fuentes en: when.google.met.wikileaks.org <<

[39] «EUR senior advisor Pandith and s/p advisor Cohen's visit to the UK, de octubre de 9-14, 2007», identificación canónica: 07LONDON4045_a, Public Library of US Diplomacy, WikiLeaks, archive.today/mxXGQ

Para más detalles sobre Jared Cohen de los archivos de WikiLeaks ver: archive.today/5fVm2

Ver también el listado de fuentes en: when.google.met.wikileaks.org **<<**

[40] Ver «Summit Against Violent Extremism (SAVE)», en la página web del Consejo de Relaciones Internacionales, archive.today/rA1tA <<

[41] Para un estudio en profundidad sobre Iniciativa de Política Exterior, ver Max Blumenthal, Rania Khalek, «How Cold War–Hungry Neocons Stage Managed RT Anchor Liz Wahl’s Resignation», *Truthdig*, 19 de marzo de 2014, archive.today/JSUHq <<

[42] «About GNF», página web de Gen Next Foundation, archive.today/p91bd
<<

[43] «AgainstViolentExtremism.org», página web de Gen Next Foundation: archive.today/Rhdtf <<

[44] «Movements.org», página web de Gen Next Foundation, archive.today/oVlqH

Es interesante destacar este extracto de un informe confidencial sobre una reunión celebrada en marzo de 2011 entre Stratfor y el «principal organizador» de Movements.org: «Cómo empezó Movements.org: [Esta parte no debe publicarse] en 2008 el gobierno de Estados Unidos llegó a la conclusión de que era preciso desarrollar una diplomacia pública a través de Internet. Jared Cohen, por entonces en el Departamento de Estado, jugó un papel crucial a la hora de poner en marcha la organización. El objetivo principal era difundir las bondades del sistema estadounidense». «[alpha] INSIGHT —US/MENA— Movements.org», correo electrónico ID 1356429 (29 de marzo de 2011), Global Intelligence Files, WikiLeaks, 4 de marzo de 2013, archive.today/PgQji

Ver también el listado de fuentes en: when.google.met.wikileaks.org <<

[45] Para más información sobre este evento, ver Joseph L. Flatley, «Being cynical: Julian Assange, Eric Schmidt, and the year's weirdest book», *Verge*, 7 de junio de 2013, archive.today/gfLEr

Ver también «The Summit: New York City, The 2008 Inaugural Alliance of Youth Movements Summit», página web de Movements.org, archive.today/H2Ox1#2008

Para una relación de los patrocinadores privados, ver «About Movements.org», página web de Movements.org, archive.today/DQo19 <<

[46] «Attendee Biographies, 3-5 de diciembre de 2008, New York City», Alliance of Youth Movements, is.gd/bLOVxT

Ver también «09 Summit, Attendee Biographies, 14-16 de octubre de 2009, Mexico City», Alliance of Youth Movements, is.gd/MddXp7

Ver también «Attendee Biographies, 9-11 de marzo de 2010, London», Movements.org, is.gd/dHTVit **<<**

[47] «The Summit: Mexico City, The 2009 Alliance For Youth Movements Summit», página web de Movements.org, archive.today/H2Ox1#2009

Y «The Summit: London, The 2010 Alliance For Youth Movements Summit», página web de Movements.org, archive.today/H2Ox1#2010 <<

[48] Hillary Rodham Clinton, «Secretary Clinton’s vídeo Message for Alliance of Youth Movements Summit», Departamento de Estado de EE. UU., 16 de octubre de 2009, archive.today/I2x6U

Ver también Hillary Rodham Clinton, «Remarks At TecMilenio University», Departamento de Estado de EE. UU., 26 de marzo de 2009, archive.today/49ACj <<

[49] Scott Shane, «Groups to Help Online Activists in Authoritarian Countries», *The New York Times*, 11 de junio de 2012, archive.today/jqq9U <<

[50] «Mission Statement», página web de Advancing Human Rights: archive.today/kBzYe

Scott Shane, «Groups to Help Online Activists in Authoritarian Countries», *The New York Times*, 11 de junio de 2012, archive.today/jqq9U <<

[51] Ibid. <<

[52] «People», página web de Advancing Human Rights, archive.today/pXmPk <<

[53] Edelman es conocido por una serie de campañas de lavado de imagen que realizó para los gigantes comerciales Big Tobacco y Walmart. La página de sourcewatch.org, que merece la pena leer entera, tiene una sección dedicada a la estrategia de Edelman para apropiarse de las causas del sector no gubernamental «Edelman dice a sus clientes que los activistas están ganando porque ‘juegan siempre al ataque, llevan su mensaje al consumidor, tienen habilidad para crear coaliciones, tienen siempre objetivos claros, se mueven a la velocidad de Internet y hablan el mismo lenguaje que los medios de comunicación’. La solución, argumenta, consiste en crear sociedades entre las ONG y las empresas. ‘Nuestra experiencia hasta la fecha es positiva’, afirman, citando ejemplos como la ‘Alianza Chiquita —Rainforest’ y ‘Home Depot— Forest Stewardship Council’. Ver «Daniel J. Edelman, Inc.», página web de SourceWatch, archive.today/APbOf

Para un listado de los patrocinadores de Movements.org, ver «About movements.org», página web de Movements.org, archive.today/NMkOy <<

[54] Para un ejemplo de la obra de Alec Ross, ver Alec Ross, Ben Scott, «Social media: power to the people?», *NATO Review*, 2011, archive.today/L6sb3 <<

[55] «Speakers», página web de Conflict in a Connected World, archive.today/Ed8rA <<

[56] El «problema principal-agente» o «dilema de agencia» se produce cuando una parte inicial, el principal, encarga a una parte aceptante, el agente, que actúe en su nombre, pero los intereses de ambas partes no están suficientemente alineados y el agente se sirve de su posición para explotar al principal. Un ejemplo clásico es cuando un abogado toma decisiones que van en su propio interés, y no en el de su cliente. <<

[57] «CAP» son las siglas de «Comité de Acción Política», un fondo de financiación de campañas políticas, utilizado a menudo para proporcionar apoyo encubierto a políticos particulares esquivando la normativa vigente al respecto, o para hacer campaña sobre un tema concreto.

Ver también los resultados de Eric y Wendy Schmidt en la página web de OpenSecrets.org, archive.today/o6hiB <<

[58] Todas las cifras de donaciones están extraídas de OpenSecrets.org (opensecrets.org/indivs) y de la Comisión Federal de Elecciones de Estados Unidos (fec.gov/finance/disclosure/norindsea.shtml). Ver los resultados registrados para Eric Schmidt en la página web de dicha comisión, archive.today/yjXoi <<

[59] «Our Funding», página web de New America Foundation, archive.today/3FnFm <<

[60] Perfil de Francis Fukuyama en la página web de New America Foundation: archive.today/6ZKk5

Perfil de Rita E. Houser en la página web de New America Foundation: archive.today/oAvJf

Perfil de Jonathan Soros en la página web de New America Foundation: archive.today/lTJy9

Perfil de Walter Russell Mead en la página web de New America Foundation: archive.today/APejM

Perfil de Helene D. Gayle en la página web de New America Foundation: archive.today/72plM

Perfil de Daniel Yergin en la página web de New America Foundation: archive.today/kQ4ys

Ver el consejo de administración completo en la página web de New America Foundation: archive.today/iBvgl <<

[61] Perfil de Anne-Marie Slaughter en la página web de New America Foundation: archive.today/yIoLP <<

[62] «Parte de la solución a la crisis en Ucrania reside en Siria. Ya es hora de que el presidente de Estados Unidos, Barack Obama, demuestre que está dispuesto y capacitado para ordenar el uso de otro tipo de fuerza distinta a los simples ataques secretos de vehículos aéreos no tripulados o a las operaciones encubiertas. El resultado modificaría sustancialmente el cálculo estratégico tanto en Damasco como en Moscú, por no hablar de Pekín y Tokio». Anne-Marie Slaughter, «Stopping Russia Starts in Syria», *Project Syndicate*, 23 de abril de 2014, archive.today/GiLng

Jared Cohen ha expresado su apoyo a Slaughter acerca de este tema en su cuenta de Twitter. Por ejemplo, el 26 de abril de 2014 publicó un mensaje en el que afirmaba que el argumento empleado en el artículo antes citado era «realmente certero», archive.today/qLyxo <<

[63] Acerca de la conferencia Bilderberg, ver Matthew Holehouse, «Bilderberg Group 2013: guest list and agenda», *The Telegraph*, 6 de junio de 2013, archive.today/PeJGc

Acerca del Consejo de Política Exterior del Departamento de Estado, ver la lista de actuales miembros del consejo de administración en la página web del Departamento de Estado: archive.today/Why8v <<

[64] Las listas de asistentes a las conferencias Bilderberg desde 2010 están disponibles en la página web de Bilderberg:

En 2011, Palantir se vió implicada en el escándalo de HBGary, al figurar como parte de un grupo de contratistas que proponían el desmantelamiento de WikiLeaks. Para más información sobre esto, ver «Trasfondo de EE. UU. contra WikiLeaks». Ver también Andy Greenberg, Ryan Mac, «How A ‘Deviant’ Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut», *Forbes*, 2 de septiembre de 2013, archive.today/ozAZ8

Los registros de los visitantes a la Casa Blanca están disponibles en esta página web: archive.today/QFQx0

Acerca de las intervenciones de Schmidt en el Foro Económico Mundial, ver Emily Young, «Davos 2014: Google’s Schmidt warning on jobs», BBC, 23 de enero de 2014, archive.today/jGl7B

Ver también Larry Elliott, «Davos debates income inequality but still invites tax avoiders», *The Guardian*, 19 de enero de 2014, archive.today/IR767 **http://www.bilderbergmeetings.org**. Eric Schmidt fue fotografiado en la edición de Bilderberg 2014 en Copenhague, se reunió con Viviane Reding, comisaria de Justicia de la Unión Europea, y con Alex Karp, consejero delegado de Palantir Technologies, una compañía de recopilación de datos que presta servicios de búsqueda e integración de datos a organismos policiales y de inteligencia, creada con financiación del fondo de capital riesgo de la CIA, In-Q-Tel. Ver Charlie Skelton, «Bilderberg conference 2014: eating our politicians for breakfast», *The Guardian*, 30 de mayo de 2014, archive.today/pUY5b <<

[65] Adrianne Jeffries, «Google’s Eric Schmidt: ‘let us celebrate capitalism’», *Verge*, 7 de marzo de 2014, archive.today/gZepE **<<**

[66] Para un ejemplo de la ambivalencia corporativa de Google en cuestiones de privacidad, ver Richard Esguerra, «Google CEO Eric Schmidt Dismisses the Importance of Privacy», Electronic Frontier Foundation, 10 de diciembre de 2009, archive.today/rwyQ7 <<

[67] Cifras válidas hasta 2013. Ver «Google Annual Search Statistics», Statistic Brain (Statistic Brain Research Institute), 1 de enero de 2014, archive.today/W7DgX <<

[68] Existe una irritante tendencia entre los abanderados de la privacidad a criticar duramente la vigilancia masiva llevada a cabo por el estado y a hacer la vista gorda ante la misma vigilancia llevada a cabo por grandes corporaciones con fines lucrativos. Esto se debe en parte a vestigios éticos de los orígenes libertarios de la defensa de la privacidad online en California, en parte a las mejores relaciones públicas con las que cuentan las corporaciones empresas tecnológicas de Silicon Valley, y en parte al hecho de que estas empresas también proporcionan la mayor parte de la financiación privada de los grupos defensores de la privacidad digital, lo que supone un conflicto de intereses.

A nivel individual, muchos de los más ardientes defensores de la privacidad tienen una adicción no reconocida a los servicios fáciles de usar y destructores de la privacidad como Gmail, Facebook, y los productos de Apple. En consecuencia, estos defensores de la privacidad a menudo pasan por alto los abusos de vigilancia de las empresas, y cuando los reconocen, como en el caso de Google, tienden a apelar a la lógica del mercado, urgiendo a las compañías a que hagan pequeñas concesiones a la privacidad del usuario para y así recuperar sus niveles de aprobación. Existe la falsa creencia de que las fuerzas del mercado garantizan que Silicon Valley sea un antagonista natural del gobierno y que desee estar del lado del público, que las corporaciones multinacionales con ánimo de lucro están más cerca del espíritu de la democracia que los organismos gubernamentales.

Muchos de estos defensores de la privacidad justifican su mayor atención a los abusos estatales argumentando que el estado disfruta de un monopolio de fuerzas coercitivas. Por ejemplo, se dice que Edward Snowden dijo que las empresas tecnológicas «no van tirando bombas nucleares a la gente». Ver Barton Gellman, «Edward Snowden, after months of NSA revelations, says his mission’s accomplished», *The Washington Post*, 23 de diciembre de 2013, archive.today/d6P8q

Esta visión resta importancia al hecho de que las corporaciones poderosas forman parte del círculo de poder existente alrededor del estado, y que disfrutan de la capacidad de desplegar su propio poder coercitivo, de la misma forma en que el estado ejerce a menudo su influencia a través de dichas corporaciones. Los movimientos para abolir la privacidad son una espada de

doble filo, y aquellos que se centran en evitar uno de esos filos acaban cortándose con el otro. <<

[69] Ver sección 7, Agradecimientos, en *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, Sergey Brin, Lawrence Page (Departamento de Ciencia Informática, Universidad de Standfor, 1998): «La investigación aquí descrita formaba parte del Proyecto Biblioteca Digital Integrada de Standfor, apoyada por la National Science Foundation, según el Acuerdo Cooperativo IRI-9411306. La financiación de este acuerdo cooperativo también corre a cargo de la DARPA y la NASA, así como de Interval Research y los socios industriales del mencionado proyecto», archive.today/tb5VL <<

[70] Michael Hayden trabaja ahora con el Chertoff Group, una empresa de consultoría que se deescribe a sí misma como una «firma de asesoramiento sobre seguridad y gestión del riesgo», fundada y dirigida por Michael Chertoff, antiguo secretario del Departamento de Seguridad Interna del presidente George W. Bush. Ver Marcus Baram, «Fear Pays: Chertoff, Ex-Security Officials Slammed For Cashing In On Government Experience», *The Huffington Post*, 23 de noviembre de 2010, actualizado el 25 de mayo de 2011, archive.today/iaM1b <<

[71] El «Conocimiento Total de Información» (en inglés, *Total Information Awareness*) fue un programa radical de la inteligencia estadounidense, instaurado tras el 11 de septiembre de 2001 y auspiciado por la DARPA, cuyo principal objetivo era la recopilación y el almacenamiento de información detallada sobre los individuos con el fin de prever su comportamiento. Este programa fue oficialmente suspendido en 2003 debido a las clamorosas protestas de la ciudadanía, pero su legado se puede entrever en recientes revelaciones de espionaje realizadas por la Agencia de Seguridad Nacional. Ver Shane Harris, «Giving In to the Surveillance State», *The New York Times*, 22 de agosto de 2012, archive.today/v4zNm <<

[72] «The Munk Debate on State Surveillance: Edward Snowden vídeo» (vídeo), Munk Debates, archive.today/zOj0t

Ver también Jane Mayer, «The Secret Sharer: Is Thomas Drake an enemy of the state?», *The New Yorker*, 23 de mayo de 2011, archive.today/pXoy9 <<

[73] «Company overview», página web de Google, archive.today/JavDC <<

[74] *Lost in the Cloud: Google and the US Government (informe)*, Consumer Watchdog's Inside Google, enero de 2011, bit.ly/1qNoHQ9

Ver también Verne Kopytoff, «Google has lots to do with intelligence», *The San Francisco Chronicle*, 30 de marzo de 2008, archive.today/VNEJi

Ver también Yasha Levine, «Oakland emails give another glimpse into the Google-Military-Surveillance Complex», *Pando Daily*, 7 de marzo de 2014, archive.today/W35WU

Ver también Yasha Levine, «Emails showing Google's closeness with the NSA Director really aren't that surprising», *Pando Daily*, 13 de mayo de 2014, archive.today/GRT18

Yasha Levine ha escrito una serie de artículos de investigación sobre los vínculos de Google con el ejército y la industria de inteligencia. Mi opinión sobre estos vínculos se basa en la investigación de Levine, que merece la pena leer en: pando.com/author/ylevine <<

[75] Yasha Levine, «Oakland emails give another glimpse into the Google-Military-Surveillance Complex», *Pando Daily*, 7 de marzo de 2014, archive.today/W35WU

Para más información sobre los vínculos de Google con la CIA, ver Noah Shachtman, «Exclusive: Google, CIA Invest in ‘Future’ of Web Monitoring», *Wired*, 28 de julio de 2010, archive.today/e0LNL <<

[76] Yasha Levine, «Oakland emails give another glimpse into the Google-Military-Surveillance Complex», *Pando Daily*, 7 de marzo de 2014, archive.today/W35WU <<

[77] Ibid. <<

[78] Ellen Nakashima, «Google to enlist NSA to help it ward off cyberattacks», *The Washington Post*, 4 de febrero de 2010, archive.today/hVTVl <<

[79] El nombre oficial de la ocupación militar estadounidense de Afganistán es bastante similar: «Operación Libertad Duradera». Ver «Infinite Justice, out — Enduring Freedom, in», BBC, 25 de septiembre de 2001, archive.today/f0fp7 <<

[80] Jason Leopold, «Exclusive: correo electrónicos reveal close Google relationship with NSA», *Al Jazeera America*, 6 de mayo de 2014, archive.today/V0fdG <<

[81] Ibid. <<

[82] «Defense Industrial Base Sector», en la página web del Departamento de Seguridad Nacional de Estados Unidos: archive.today/Y7Z23 <<

[83] Ver «Top Spenders» en «Influence and Lobbying» en la página web OpenSecrets.org: archive.today/xQyui

Ver también Tom Hamburger, «Google, once disdainful of lobbying, now a master of Washington influence», *The Washington Post*, 13 de abril de 2014, archive.today/oil7k <<

[84] Sy Hersh ha escrito dos artículos sobre la funesta «intervención» de Obama en Siria. Ver Seymour M. Hersh, «Whose Sarin?», *London Review of Books*, 19 de diciembre de 2013, archive.today/THPGh

Ver también Seymour M. Hersh, «The Red Line and the Rat Line», *London Review of Books*, 17 de abril de 2014, archive.today/qp5jB **<<**

[85] Puede consultarse una imagen de dicha página en archive.today/Q6uq8

Google se enorgullece explícitamente de mantener su página principal libre de toda interferencia, hasta el punto de que su pureza y sacralidad están incluidas en su manifiesto corporativo: «La interfaz de nuestra página de inicio es clara y simple, y las páginas buscadas cargan instantáneamente. La ubicación en las páginas de resultados de búsqueda no está en venta para ningún individuo o empresa, y la publicidad no solo está claramente señalada como tal, sino que ofrece contenidos relevantes para cada búsqueda y no distrae del objetivo principal». Ver «Ten things we know to be true», página web de Google, archive.today/s7v9B#selection-243.52-243.277

Las contadas ocasiones en las que Google añade una sola línea a su página de búsqueda para publicitar sus propios proyectos, como el buscador Chrome, se convierten automáticamente en noticia. Ver Cade Metz, «Google smears Chrome on ‘sacred’ home page», *Register*, 9 de septiembre de 2008, archive.today/kfneV

Ver también Hayley Tsukayama, «Google advertises Nexus 7 on home page», *The Washington Post*, 28 de agosto de 2012, archive.today/QYfBV <<

[86] Thomas Friedman ha publicado numerosas columnas de opinión ensalzando las virtudes de su «centrismo radical», como por ejemplo «Make Way for the Radical Center», *The New York Times*, 23 de julio de 2011, archive.today/IZzhb **<<**

[87] Thomas Friedman, «A Manifesto for the Fast World», *The New York Times*, 28 de marzo de 1999, archive.today/aQHvy **<<**

[88] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 98.

Google está muy comprometido con su ambición. Desde comienzos de 2013, Google ha comprado nueve empresas de robótica experimental e inteligencia artificial y las ha puesto a trabajar con un objetivo no declarado bajo las órdenes de Andy Rubin, antiguo director de la división Android de Google. Ver John Markoff, «Google Puts Money on Robots, Using the Man Behind Android», *The New York Times*, 4 de diciembre de 2013, archive.today/Izr7B

Ver también Adam Clark Estes, «Meet Google's Robot Army. It's Growing», *Gizmodo*, 27 de enero de 2014, archive.today/mN2GF

Dos de las adquisiciones de Google participaban como competidores en el Desafío de Robótica de la DARPA, una competición diseñada por la Agencia de Proyectos de Investigación Avanzada de Defensa, con generosas donaciones de apoyo financiero a los contendientes por parte del Pentágono. Una de estas dos, Schaft Inc, una compañía japonesa, era la favorita para alzarse con el triunfo en esta competición gracias a su proyecto: un robot humanoide bípedo inmune a cualquier tipo de radiación, capaz de subir escaleras, abrir puertas y desplazarse por terrenos accidentados. La otra, Boston Dynamics, estaba especializada en la producción de robots militares capaces de caminar, correr y reptar, destinados al Departamento de Defensa; el producto de Boston Dynamics más conocido se llama «BigDog», un transporte de apoyo del tamaño de perro grande (de ahí el nombre) que hay que verlo para creerlo (en YouTube: is.gd/xOYFdY). Ver Breezy Smoak, «Google's Schaft robot wins DARPA rescue challenge», *Electronic Products*, 23 de diciembre de 2013, archive.today/M7L6a

Ver también John Markoff, «Google Adds to Its Menagerie of Robots», *The New York Times*, 14 de diciembre de 2013, archive.today/cqBX4

El poder real de Google como compañía fabricante de vehículos no tripulados es que su colección de datos de navegación no tiene rival, si se incluye toda la información asociada con Google Maps y la localización de alrededor de 1000 millones de personas. Sin embargo, no debe asumirse que, una vez recopilada, esta información se va a usar siempre para fines inocuos: los datos de mapeado recogidos por el proyecto Google Street View, para cuya

elaboración enviaron innumerables coches a recorrer las calles de otras tantas ciudades de todo el mundo, pueden resultar cruciales en el futuro a la hora de dirigir robots militares o policiales por esas mismas calles. <<

[89] Una utopía que en ocasiones roza la megalomanía. El consejero delegado de Google Larry Page, por ejemplo, ha invocado públicamente la imagen de microestados similares a parques jurásicos en los que Google estuviera exenta de cumplir las leyes nacionales y pudiera progresar sin impedimentos. «Una ley […] no puede ser aplicable si tiene cincuenta años, ya que fue creada antes que Internet. […] Tal vez podríamos separar una pequeña porción del mundo, […] un entorno en el que la gente pueda probar cosas nuevas. Pienso que, como tecnólogos, deberíamos tener unos espacios seguros en los que probar estas cosas nuevas y estudiar su efecto en la sociedad, el efecto sobre las personas, sin tener que desplegarlas necesariamente al resto del mundo». Ver Sean Gallagher, «Larry Page wants you to stop worrying and let him fix the world», *Ars Technica*, 20 de mayo de 2013, archive.today/kHYcB **<<**

[90] La conocida compañía mercenaria Blackwater, famosa por matar civiles iraquíes, fue rebautizada como Xe Services en 2009 y posteriormente como Academi en 2011. Ver Jeremy Scahill, *Blackwater: el auge del ejército mercenario más poderoso del mundo* (Ediciones Paidós Ibérica, 2008). <<

[91] Desde el principio, el éxito de Google se basó en la vigilancia comercial de civiles a través de «servicios»: búsqueda por Internet, correo electrónico, redes sociales, etcétera, pero su desarrollo en los últimos años ha ampliado su ámbito de vigilancia pasando a controlar los teléfonos móviles y las tablets. El éxito del sistema operativo móvil de Google, Android, lanzado en 2008, le ha otorgado el 80 % del mercado de los smartphones. El propio Google afirma que hay registrados más de mil millones de dispositivos Android, y el ritmo de nuevos registros ha superado el millón diario. Ver «Q1 2014 Smartphone OS Results: Android Dominates High Growth Developing Markets», *ABIresearch*, 6 de mayo de 2014, archive.today/cTeRY

Ver también «Android, the world's most popular mobile platform», en la página web de Android Developers: archive.today/5y8oe

A través de Android, Google está en disposición de controlar los dispositivos que millones de personas llevan consigo en su vida diaria y utilizan para conectarse a Internet. Cada uno de estos dispositivos proporciona a la compañía estadísticas de uso, localización y otros datos, lo que a su vez le permite tener un poder sin precedentes a la hora de supervisar e influir en las actividades de su base de usuarios, tanto a través de la red como en sus actividades habituales. Otros proyectos de Google como el «Proyecto Glass» y el «Proyecto Tango» aspiran a incrementar aún más su omnipresencia, ampliando aún más sus capacidades de vigilancia. Ver Jay Yarow, «This Chart Shows Google's Incredible Domination Of The World's Computing Platforms», *Business Insider*, 28 de marzo de 2014, archive.today/BTDJJ

Ver también Yasha Levine, «Surveillance Valley has put a billion bugs in a billion pockets», *Pando Daily*, 7 de febrero de 2014, archive.today/TA7sq

Ver también Jacob Kastrenakes, «Google announces Project Tango, a smartphone that can map the world around it», *Verge*, 20 de febrero de 2014, archive.today/XLLvc

Ver también Edward Champion, «Thirty-Five Arguments Against Google Glass», *Reluctant Habits*, 14 de marzo de 2013, archive.today/UUJ4n

Google también aspira a convertirse en proveedor de Internet. El «Proyecto Loon» tiene como objetivo proporcionar acceso a Internet a las poblaciones aisladas del sur del planeta, mediante emisores inalámbricos de señales

ubicados en flotas de globos aerostáticos de gran altitud y vehículos aéreos no tripulados, para lo cual ha adquirido recientemente dos compañías especializadas en estos vehículos: Titan Aerospace y Makani Power. Facebook, que pujó frente a Google por hacerse con Titan Aerospace, tiene aspiraciones similares, pues a su vez ha comprado otra compañía especialista británica llamada Ascenta. Ver Adi Robertson, «Google X 'moonshots lab' buys flying wind turbine company Makani Power», *Verge*, 22 de mayo de 2013, archive.today/gsnio

Ver también la página web del Proyecto Loon: archive.today/4ok7L

Ver también Sean Hollister, «Google nabs drone company Facebook allegedly wanted to buy», *Verge*, 14 de abril de 2014, archive.today/hc0kr **<<**

[92] Para un ejemplo de la preocupación europea, ver Mathias Döpfner, «Why we fear Google», *Frankfurter Allgemeine*, 17 de abril de 2014, archive.today/LTL6l <<

[93] La vigilancia policial sigue activa aún en el momento de escribir este libro, lo que hasta el momento ha supuesto un coste de alrededor de 7,5 millones de euros para el departamento del Tesoro de Reino Unido. Ver Martin Robinson, «Julian Assange has cost Britain £6m as policing bill to guard Ecuadorian embassy where WikiLeaks fugitive is hiding soars», *Mail Online*, 25 de abril de 2014, archive.today/RwwyH **<<**

[94] Madeleine Albright es conocida por promover la imposición de sanciones contra Irak, la campaña de bombardeos de la OTAN contra Yugoslavia en 1999, y la expansión de la OTAN hasta las fronteras de Rusia. En una famosa declaración, afirmó que la muerte de 500 000 niños iraquíes como resultado del régimen de sanciones había «valido la pena». Ver «Madeleine Albright says 500,000 dead Iraqi Children was ‘worth it’… wins Presidential Medal of Freedom from Obama» (vídeo), subido a Internet el 2 de mayo de 2012, youtu.be/omnskeu-puE <<

[95] Para cuando mi reseña salió publicada, el experto en tecnología Evgeny Morozov —uno de los pocos escritores que aún tienen algo interesante que decir acerca de la intersección entre tecnología y política— ya había publicado su propia reseña del libro en la revista quincenal *The New Republic*. Merece mucho la pena leer atentamente su artículo, así como su feroz diatriba sobre la estética «purista» de Apple, su cáustica crítica de la cultura existente en torno al circuito de conferencias TED, y su disección de la jerga de Silicon Valley, que progresivamente ha ido invadiendo el lenguaje político (el «discurso público 2.0»). Los escritos de Morozov me han ayudado a formar mi perspectiva sobre algunos de estos temas.

Sobre el libro *The New Digital Age*, ver Evgeny Morozov, «Future Shlock», *The New Republic*, 27 de mayo de 2013, archive.today/k3N7O

Sobre Apple, ver Evgeny Morozov, «Form and Fortune», *The New Republic*, 22 de febrero de 2012, archive.today/P2Vog

Sobre TED, ver Evgeny Morozov, «The Naked and the TED», *The New Republic*, 2 de agosto de 2012, archive.today/yTy2Q

Sobre la jerga de Silicon Valley, ver Evgeny Morozov, «The Meme Hustler», *Baffler*, número 22, 2013, archive.today/fQhqW <<

[96] Julian Assange, «The Banality of ‘Don’t Be Evil’», *The New York Times*, 2 de junio de 2013, archive.today/kxMZM **<<**

[97] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), pp. 8–11. <<

[98] Este respaldo puede comprobarse en la página web del Consejo de Relaciones Internacionales, donde *The New Digital Age* cuenta con su propio apartado, archive.today/rQtyh <<

[99] Donald Melanson, «Eric Schmidt: Google now at 1.5 million Android activations per day», *Engadget*, 16 de abril de 2013, archive.today/wJh4i **<<**

[100] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 122. <<

[101] Ibid., p. 122, p. 128. <<

[102] Ibid., p. 149. <<

[103] Ibid., p. 144. <<

[104] Ibid., p. 133. <<

[105] Ibid., p. 133. <<

[106] Ibid., p. 144. <<

[107] Ibid., todo el libro; por ejemplo, p.166, pp. 96-97, etcétera. <<

[108] Ibid., p. 151. <<

[109] Ibid., p. 152, p. 162. <<

[110] Ibid., p. 155. <<

[111] Ibid., p. 162. <<

[112] Julian Assange con Jacob Appelbaum, Andy Müller-Maguhn, y Jérémie Zimmermann, *Cypherpunks: la libertad y el futuro de Internet* (Ediciones Deusto, 2013). <<

[113] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), pp. 57–64. <<

[114] Ibid., pp. 59–63. <<

[115] La «norma del nombre real» de Google, que establecía que su uso bajo cualquier nombre que no fuese el nombre legal y completo del usuario se consideraría una violación del contrato, fue introducida por primera vez en 2011, con el apoyo explícito y público de Eric Schmidt. Ver Matt Rosoff, «Google+ Isn't Just A Social Network, It's An 'Identity Service'», *Business Insider*, 28 de agosto de 2011, archive.today/G5iRE

Esta normativa provocó inmediatamente lo que dio en llamarse como las «Nymwars», una prolongada controversia entre comentaristas, blogueros y usuarios de redes sociales sobre la importancia del anonimato en Internet. Ver Jillian York, «A Case for Pseudonyms», Electronic Frontier Foundation, 29 de julio de 2011, archive.today/LhInw

Ver también Eva Galperin, «2011 in Review: Nymwars», Electronic Frontier Foundation, 26 de diciembre de 2011, archive.today/bEYJd <<

[116] Palabras textuales de Schmidt y Cohen. Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 75.

Con estas palabras están parafraseando a William Dobson, *The Dictator's Learning Curve: Inside the Global Battle for Democracy* (Doubleday, 2012). <<

[117] A principios de mayo de 2013 salió a la luz que, como parte de una investigación sobre la fuente de un asunto de seguridad nacional, el Departamento de Justicia de Estados Unidos había solicitado en secreto a la compañía de telecomunicaciones Verizon los registros de dos meses de llamadas telefónicas de veinte reporteros de Associated Press, acción que fue ampliamente condenada como un ataque a la libertad de prensa. Ver Mark Sherman, «US government secretly obtained Associated Press phone records», Associated Press, 13 de mayo de 2013, archive.today/vyuNP

Más o menos al mismo tiempo, *The Washington Post* informó de que en el curso de otra investigación criminal realizada por el Departamento de Justicia sobre una fuente periodística, el FBI había acumulado una gran cantidad de datos confidenciales sobre el reportero de Fox News James Rosen. Documentos de la acusación final de espionaje provenientes de la fuente del gobierno, Stephen Jim-Woo Kim, revelaron que el Departamento de Justicia había clasificado a Rosen como «co-conspirador no acusado» y consideraba que su riesgo de fuga era elevado, lo que básicamente implicaba que la práctica básica del periodismo pasaba a considerarse como actividad criminal. Ver Ann E. Marimow, «A rare peek into a Justice Department leak probe», *The Washington Post*, 20 de mayo de 2013, archive.today/LkTLR

Ver también «Justice Department affidavit labels Fox News journalist as possible ‘co-conspirator’», Fox News, 20 de mayo de 2013, archive.today/HBsA4 <<

[118] La referencia a los «fundadores, propietarios o gerentes» de WikiLeaks procede de la declaración judicial del agente especial Mark Mander, de la Unidad de Investigación de Crímenes Informáticos del Ejército de Estados Unidos, efectuada durante las audiencias previas al juicio de Chelsea Manning <<

[119] Mi reseña fue a la prensa en vísperas del juicio a Chelsea Manning, después de 1103 días de confinamiento previo. Por entonces, Chelsea Manning aún era conocida como Bradley Manning, su nombre antes de cambiarse de sexo. Ver Chelsea E. Manning, «Chelsea Manning announces gender transition—full statement», *The Guardian*, 22 de agosto de 2013, archive.today/eMCdr

Chelsea Manning fue hallada culpable y condenada a treinta y cinco años de cárcel. Para más información sobre su juicio, ver «Trasfondo de EE. UU. contra WikiLeaks», página 205 <<

[120] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 98. <<

[121] «About the author» en Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013). **<<**

[122] Ibid. <<

[123] El perfil como personal del Consejo de Relaciones Internacionales de Shield está disponible en: **http://www.foreignaffairs.com**, archive.today/YSNrj <<

[124] El perfil como personal del International Crisis Group de Malcomson está disponible en: **http://www.crisisgroup.org**, archive.today/ETYXp **<<**

[125] La grabación de audio está disponible en: **http://www.wikileaks.org/Transcript-Meeting-Assange-Schmidt.html** <<

[126] Finalmente la publicación tuvo lugar en abril de 2013, con el título *The New Digital Age: Reshaping the Future of People, Nations and Business*. **<<**

[127] *The New Digital Age* fue finalmente publicado sin la prometida consulta. Esta transcripción fue elaborada por mi equipo. <<

[128] Tor es un software gratuito que permite a sus usuarios navegar por Internet de forma anónima, y su primer diseño fue patrocinado por el laboratorio de investigación de la Marina de Estados Unidos. Ver la página web del proyecto Tor: **http://www.torproject.org/about/overview <<**

[129] Dios de la mitología nórdica, al igual que Thor. <<

[130] Para cualquier información sobre WikiLeaks, ver su página web: wikileaks.org <<

[131] En este caso, lo que se entiende por «no lineal» es el hecho de que el ritmo de difusión de la información no es constante, sino que se va acelerando a medida que se va extendiendo entre la población. Por ejemplo, si un día una persona revela una idea a dos personas, al día siguiente esas tres personas la revelan a su vez a otras dos cada una, y así sucesivamente, al primer día lo sabrán tres personas, al segundo nueve, al séptimo 2187, y al cabo de veintiún días lo sabrá toda la población mundial (dada la actual cifra oficial de 7100 millones de habitantes). Literalmente, «no lineal» significa que «no puede representarse por medio de una línea recta». <<

[132] El «cuarto poder» es un término informal que alude a cualquier grupo externo a organismos gubernamentales o políticos que tiene influencia sobre los mismos, normalmente referido a la prensa. <<

[133] Para una representación visual de la pirámide de la censura, ver Marienna Pope-Weidemann, «Cypherpunks: Freedom and the Future of the Internet» (reseña), *Counterfire*, 13 de septiembre de 2013, archive.today/Oyczc

Para un mayor desarrollo de esta idea, ver Julian Assange con Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann, *Cypherpunks: la libertad y el futuro en Internet* (Ediciones Deusto, 2013). **<<**

[134] «Frente distribuido» es una descripción técnica. El «frente» de una página web es la parte visible cuando se visita con un navegador de Internet. En la mayoría de las páginas web de nueva creación, el frente y la parte trasera se encuentran en la misma ubicación física, lo cual significa que son más fáciles de censurar, puesto que únicamente hay un punto débil. WikiLeaks fue diseñada específicamente para lidiar con la censura, por lo que usó un modelo diferente, con su parte trasera oculta y con su frente distribuido en muchos ordenadores diferentes. Esto supone que incluso si uno de esos ordenadores que albergan el «frente» de la página es atacado y eliminado, aún existirían muchas otras copias, por lo que la página web seguiría disponible al público. Además, la «parte trasera» de la página sigue estando oculta, y se pueden crear fácilmente todos los nuevos «frentes» que hagan falta. <<

[135] Un «nombre de dominio» es un nombre legible para los humanos de una página web, como «wikileaks.org» o «whitehouse.gov». A todos los dispositivos conectados a Internet se les asigna una dirección numérica, conocida como dirección IP, y todas las páginas web de Internet pueden ser visitadas con esa dirección IP. Por ejemplo, «195.35.109.44» es una dirección IP de la página de WikiLeaks (una de muchas). El problema es que estas direcciones IP son difíciles de recordar, por lo que para facilitar la memorización se inventó el «sistema de nombres de dominio» (DNS, por sus siglas en ingles): un sistema para vincular «nombres de dominio» a direcciones IP.

A diferencia de las direcciones IP, que se asignan automáticamente cuando se conecta un dispositivo a la red, cualquiera puede ser propietario de un nombre de dominio de su elección registrándolo en «registro público de nombres de dominio» y pagando una pequeña tarifa. Todos los nombres de dominio pasan a formar parte de un directorio global —similar al directorio telefónico— que vincula cada nombre de dominio a la dirección IP real de cada página web. Cada vez que se teclea «wikileaks.org» en un navegador, lo primero que hace este navegador es hacer una «búsqueda», que consiste en contactar con un servidor DNS, que contiene una copia del directorio global, y rastrea el nombre de dominio «wikileaks.org» para encontrar la correspondiente dirección IP, y entonces cargar la página web a partir de esta IP. Cuando un nombre de dominio se traduce con éxito a una dirección IP, se dice que ha «resuelto».

Un «ataque a un DNS» es un intento de eliminar la página web interfiriendo en el directorio que vincula al nombre de dominio con la dirección IP, de forma que deje de resolver. Sin embargo, al igual que existen muchos directorios telefónicos diferentes, también existen muchos servidores DNS diferentes; por ello, si se es capaz de cambiar rápidamente de DNS, es posible defenderse de los efectos de un ataque a un DNS y garantizar que la página web esté siempre accesible. <<

[136] En abstracto, un “sistema de memoria caché” es un sistema rápido que en principio no contiene información, pero que está conectado a un sistema lento que sí tiene. Cuando se pide información a este tipo de sistema, inicialmente traslada la petición a un sistema lento, reenvía la respuesta y se queda con una copia, por lo que cuando se le vuelve a pedir la misma información se limita a enviar la copia ya realizada.

WikiLeaks utiliza abundante tecnología para ocultar y codificar su información que puede ralentizar el camino hacia la “parte trasera”, donde se genera el contenido. En este contexto, un sistema de memoria caché está diseñado para acelerar el sistema en su conjunto y hacerlo más sencillo de usar, incrementando la velocidad de respuesta ante peticiones repetitivas, que son la mayoría. <<

[137] Un «servidor oculto», en este contexto, es aquel servidor que no es accesible mediante Internet convencional. WikiLeaks utilizaba un *software* personalizado para ocultar algunas de sus páginas, de forma que fuesen inaccesibles a la mayor parte de Internet.

La «parte trasera» de WikiLeaks —esto es, el *software* que produce la página web de WikiLeaks— estaba oculto, y desde esa «parte trasera» oculta el contenido era canalizado hacia el frente a través de «pasadizos de la red Tor», es decir, sirviéndose de la red oculta y codificada del sistema Tor para canalizar el contenido a los servidores, donde la gente pudiese acceder a él.

El concepto es similar al de «servicios ocultos de Tor». Ver la página web del Proyecto Tor: archive.today/tmQ5y <<

[138] «DNS» significa «domain name system» («*sistema de nombre de dominio*»). Para una explicación más detallada, ver nota al pie 15, «nombre de dominio». <<

[139] Un «nodo frontal sacrificable» no es más que una copia de la parte frontal de una página web (ver nota al pie 14, en «frente distribuido»), copia que se espera que entre en el punto de mira de aquellas entidades que desean censurar WikiLeaks. La creación de los nodos frontales es fácil y barata, y pueden ser copiados rápidamente desde un servidor oculto. El atacante puede centrar sus esfuerzos en estos nodos frontales sacrificables, pero cuando consiguen cortar uno aparecen más en su lugar, por lo que la censura es cara e inútil. <<

[140] A mediados de la década de 2000, Suecia estaba considerada como un paraíso por los usuarios de Internet, con una tasa alta de conectividad (cerca del 90 % de los hogares suecos tenían conexión a Internet) y unas políticas gubernamentales muy favorables a la tecnología. Muchos servicios de Internet que se veían amenazados por la censura escogían Suecia como refugio electrónico. Por desgracia, a medida que se incrementaban los perfiles de servicios que se trasladaban a Suecia, comenzaron a surgir conflictos entre esta característica de Suecia y sus relaciones geopolíticas, especialmente con Estados Unidos. Esto condujo a una serie de enérgicas medidas (por ejemplo, el juicio Pirate Bay) provocadas por la presión de la Casa Blanca, tal y como demuestran los comunicados publicados por WikiLeaks y la consiguiente huida de estos servicios. Suecia tiene una población de solo nueve millones de personas, está aislada geográficamente y cerca de una nuevamente emergente Rusia. En última instancia, el país carecía del peso y de la influencia geopolítica como para arriesgarse a ofender a su principal aliado militar, Estados Unidos. Ver Rick Falkvinge, «Cable Reveals Extent Of Lapdoggery From Swedish Govt On Copyright Monopoly», *Falkvinge & co. on Infopolicy*, 5 de septiembre de 2011, archive.today/r9jb4 <<

[141] «Muy pocos saltos» significa que no había muchas transiciones entre los nodos frontales y el lector. <<

[142] Un «ataque de denegación de servicio» (en inglés, DoS) es un intento de impedir el acceso a una página web mediante el envío de tantas peticiones de acceso que la página es incapaz de responder a todas. Esta es una forma de censurar una página centrándose en la fuente y desactivándola de forma efectiva. <<

[143] El «filtrado», o control de contenido, se produce cuando un proveedor de Internet bloquea el acceso a una página web determinada. Esta forma de censura básicamente consiste en ubicarse entre la página y los usuarios e interferir de manera selectiva en el tráfico. <<

[144] En este contexto, el «filtrado de nivel DNS-IP» implicaba que el sistema de censura chino bloqueaba efectivamente las direcciones IP en los servidores DNS que eran las que resolvían el nombre de dominio «wikileaks.org» en las direcciones IP de la página web de WikiLeaks. WikiLeaks logró contrarrestar esto utilizando unos servidores DNS muy grandes que contenían hasta medio millón de otros nombres de dominio.

Al bloquear las direcciones IP de estos servidores DNS, los censores chinos causaban un daño colateral masivo, pues junto con WikiLeaks censuraban también cientos de miles de otras páginas. El posible malestar político que hubiese provocado tal acción probablemente disuadió a los censores de llevarla a cabo. <<

[145] El «filtrado de contenido» implica el bloqueo de una página web basándose en el contenido de la misma, en lugar de limitarse a bloquear el acceso a un nombre de dominio o dirección IP concreta; por ejemplo, bloqueando todas las páginas web que mencionen a WikiLeaks. <<

[146] «HTTPS» son las siglas de «Hypertext Transfer Protocol Secure», un «Protocolo de Transmisión Segura de Hipertexto» que codifica las conexiones entre un navegador y un servidor, o, en este caso, entre el navegador de un usuario en China y el servidor de la página web de WikiLeaks. Los HTTPS impidieron que el gobierno chino examinase los datos transferidos entre el navegador y el servidor, y por tanto impidió su filtrado. Sin embargo, desde entonces se han desarrollado métodos de ataque a este protocolo. <<

[147] «Cambiar las IP» significa cambiar las direcciones IP. El sistema de censura chino funcionaba con una lista de direcciones IP que debían bloquearse. Cambiando rápidamente a nuevas direcciones IP, la página de WikiLeaks podía seguir estando disponible a los usuarios chinos, al menos hasta que los censores actualizaban su lista y bloqueaban las nuevas direcciones IP. <<

[148] Un bloque IP es una serie de direcciones IP consecutivas, asignadas habitualmente como un paquete único a una organización o a un departamento gubernamental que desea conectar muchos dispositivos a Internet, y por tanto necesita un gran número de estas direcciones. En este caso, los ordenadores ubicados dentro de China intentaban periódicamente buscar las direcciones IP cuyo nombre de dominio era «wikileaks.org», y el hecho de que todos estos ordenadores estuviesen dentro del mismo bloque IP mostraba que se trataba de una única organización china. Esto fue la primera pista de que se trataba del sistema censor chino, y la pista fue confirmada en posteriores investigaciones. <<

[149] Con el fin de bloquear WikiLeaks en China, el sistema censor chino tenía que usar el sistema de nombres de dominio para rastrear las direcciones IP en busca de los servidores de WikiLeaks, para luego bloquearlos. No obstante, la búsqueda de direcciones IP de WikiLeaks era tan regular que era posible distinguirla del tráfico normal de usuarios, por lo que también era posible proporcionar a los censores información falsa acerca de cuáles de los servidores estaban controlados por WikiLeaks, y lo que hacían era bloquear servidores falsos en lugar de los reales. Los usuarios normales de la página web de WikiLeaks en China no se vieron afectados. **<<**

[150] Lo cual provocó que el Ministerio de Seguridad Pública, encargado de gestionar el sistema censor chino, se añadiese a *sí mismo* a la lista de páginas a censurar. <<

[151] El general Sitiveni Ligamamada Rabuka lideró dos golpes de estado en Fiji en 1987 para derrocar al gobierno étnico dominado por indios que había sido elegido democráticamente, y reemplazarlo por otro compuesto de indígenas locales. <<

[152] Durante toda la conversación se alude a objetos situados encima de la mesa para ilustrar conceptos a través de sus relaciones espaciales. <<

[153] «URL» son las siglas de «uniform resource locator» («*localizador de recursos uniformes*»), y es otra forma sencilla de dar nombre a las direcciones de páginas web, como **https://www.wikileaks.org/donate <<**

[154] En este contexto, el «terreno de lo platónico» alude al universo de los conocimientos posibles. La frase tiene su origen en la teoría de las formas o teoría de las ideas de Platón, pero la exploración más atractiva sobre el tema es el famoso relato corto «La biblioteca de Babel», del escritor argentino Jorge Luis Borges (1899-1986), disponible en archive.today/Fm4fM (inglés) y en **http://www.literaberinto.com/vueltamundo/bibliotecaborges.htm** (español). **<<**

[155] Ver la sección dedicada a Nadhmi Auchi en WikiLeaks, archive.today/BkT0D <<

[156] El estrangulador de Boston fue un asesino en serie que mató a 13 mujeres en esta ciudad de Massachusetts a comienzos de los años 60. Supuestamente, en muchos de sus crímenes se hizo pasar por un vendedor ambulante puerta por puerta para engañar a las mujeres y que le dejasen entrar en sus apartamentos. <<

[157] El círculo de la historia se cerró cuando la magistrada francesa que se encargó de aquel asunto, Eva Joly, investigó la corrupción de los bancos islandeses, se presentó a las elecciones presidenciales de 2012 en Francia, perdió, fue elegida diputada del Parlamento Europeo, y posteriormente se presentó en la embajada ecuatoriana en Londres, donde resido, para intentar encontrar una solución a mis cuatro años de detención sin cargos en Reino Unido. <<

[158] WikiLeaks los ha reincorporado al archivo histórico. Ver archive.today/oOCks <<

[159] George Orwell, *[1984*, Ediciones Destino, 2010]. <<

[160] En este caso, «bits» se utiliza en el sentido de información: «esos bits», «esa información». <<

[161] «ISP» son las siglas de «internet service provider» («*proveedor de servicio de Internet*»). En este contexto, un ISP es una compañía que proporciona enlaces de comunicación o espacio de servidor para crear una página web. A la hora de elegir un ISP para una página como WikiLeaks, es necesario considerar algunas cuestiones muy importantes, como por ejemplo: «¿Te apoyará este ISP en tu lucha contra la censura, o te censurará él mismo?» <<

[162] Las Islas Turcas y Caicos es un territorio británico de ultramar ubicado en el Caribe. <<

[163] Dado que las Islas Turcas y Caicos son territorio británico, la Corona —la monarquía británica— es la propietaria formal del terreno público. **<<**

[164] «The Pirate Bay» («*La bahía pirata*») es un ISP creado en 2003 por mi amigo Gottfrid Svartholm (apodado «anakata»), quien también trabajó para WikiLeaks como asesor. Fue procesado en Suecia por presiones de Estados Unidos (tal y como muestran los comunicados de WikiLeaks), más tarde detenido en Camboya por el servicio de inteligencia sueco SAPO, juzgado nuevamente en Suecia y después extraditado a Dinamarca, donde actualmente espera un nuevo juicio. The Pirate Bay es un rastreador del estilo de BitTorrent, que permite compartir archivos grandes entre ordenadores conectados a Internet coordinando la comunicación entre ellos, y su página web, bloqueada en muchos sitios, es

Ver también Rick Falkvinge, «Cable Reveals Extent Of Lapdoggery From Swedish Govt On Copyright Monopoly», *Falkvinge & co. on Infopolicy*, 5 de septiembre de 2011, archive.today/r9jb4 **http://www.thepiratebay.se**. Ver Kristina Svartholm, «Gottfrid Svartholm Warg: a year of his life from his mother's perspective», WikiLeaks, 18 de agosto de 2013, is.gd/h2MeG4 **<<**

[165] Además de su asociación con Pirate Bay y PRQ, Gottfrid Svartholm fue un asesor de WikiLeaks que colaboró en la publicación del vídeo *Daño Colateral* (sobre este tema, ver nota al pie 237; el vídeo está disponible en youtu.be/5rXPrfnU3G0 y también en **https://www.youtube.com/watch?v=Wfzz12LzMuQ** con subtítulos en español). Tras su publicación, la mayoría de los que aparecen en los créditos de este vídeo han sufrido acoso de un modo u otro, y el propio Gottfrid se ha tenido que enfrentar a prolongadas batallas legales. Para más información y documentación sobre su proceso legal, ver «Prosecution and prison documents for Pirate-Bay founder Gottfrid Svartholm Warg (alias Anakata)», WikiLeaks, 19 de mayo de 2013, archive.today/aOsLB <<

[166] Para más información sobre PRQ, ver su página web:

Para más información sobre Bahnhof, ver su página web: **http://www.bahnhof.net http://www.prq.se <<**

[167] El Centro Kavkaz informa desde Chechenia desde una perspectiva islámica. Para más información, ver archive.today/djebS

Actualmente, el Instituto Rick A. Ross para el Estudio de Cultos Destructivos, Grupos Controvertidos y Movimientos se conoce como el Instituto Educativo sobre Cultos. Para más información, ver archive.today/8PQ4K <<

[168] *Malasia Today* es un popular blog de noticias malayo. En 2008, el gobierno del país lo bloqueó temporalmente, y su fundador, Raja Petra Kamarudin, pasó varios meses en la cárcel. Para más información, ver archive.today/6S0QZ <<

[169] Un «espejo» es una réplica exacta de una página web. <<

[170] Una «copia de seguridad codificada» es una copia del material que se mantiene por separado en un lugar seguro por si le ocurre algo al original. Esta copia se codifica mediante una clave o una contraseña, de forma que solo pueden leerla aquellos que tengan acceso a dicha clave o contraseña. <<

[171] «FTP» son las siglas de «file transfer protocol» («*protocolo de transferencia de archivos*»), uno de los métodos más utilizados para enviar archivos por Internet. No es un método empleado por WikiLeaks, pero en este caso Schmidt lo utiliza como ejemplo de envío de datos por Internet. <<

[172] Un «ataque contra los extremos» (p.ej., *software* espía implantado por una agencia de inteligencia, o un virus informático) es un ataque dirigido a comprometer uno de los «puntos extremos», es decir, o bien el ordenador que envía la información, o bien el que la recibe. Cuando dos ordenadores se comunican mediante un código bien desarrollado e implementado, se podrá interceptar el mensaje, pero será imposible poder leerlo. La única solución en este caso es realizar un ataque contra un extremo antes de su codificación o después de su descodificación. <<

[173] Esto significa que no tienes que preocuparte de si las compañías y sistemas de telecomunicación que transfieren o almacenan la información la modifican de alguna forma. <<

[174] Una «red inundada» distribuye la información haciendo que cada servidor envíe la información nueva a todos los demás servidores que estén conectados a él. Este método se llama así porque es similar a un río que se desborda e inunda cada afluente conectado. Siempre y cuando no haya servidores aislados, todos y cada uno de ellos acabarán recibiendo la información tarde o temprano, puesto que se cubren todas las posibles vías, y por tanto también la vía más rápida. <<

[175] Un «algoritmo hash» o una «función hash» es una fórmula que convierte cualquier conjunto de datos, del tamaño que sea, y lo convierte en «picadillo» (en inglés, «hash»): un código (representado por una secuencia de caracteres de longitud fija) que puede usarse para representar el conjunto original de datos. Un ejemplo de un hash poco seguro que se ve todos los días es el uso de acrónimos para representar nombres que son demasiado largos para su uso práctico, como por ejemplo «OTAN» en lugar de «Organización del Tratado del Atlántico Norte». En este caso, la fórmula es muy sencilla: «tomar la primera letra de cada palabra».

Las «funciones hash» más típicas son fórmulas matemáticas que toman una información del tamaño que sea y la «pican», reduciéndola a un «hash» o «picadillo» de extensión reducida y fija. Un hash seguro utiliza una fórmula muy compleja, tanto que, si bien un ordenador de potencia modesta puede crear un hash a partir de una información original, ni siquiera el ordenador más potente del mundo puede hacer la operación opuesta, esto es, crear una información original que coincida con un hash concreto. Por ejemplo, volviendo al acrónimo OTAN, no podría encontrar «Organización del Tratado del Atlántico Norte» ni ninguna otra alternativa, como «Obama Trata de Arreglar la Nación». Por supuesto, «tomar la primera letra de cada palabra» no es una función hash segura, puesto que es fácil pasar del hash a la información que lo origina, pero no es este el caso de las funciones hash más seguras.

Un hash seguro está compuesto por varias decenas de caracteres, en lugar de los cuatro del ejemplo utilizado, por lo que resulta muy difícil que un ser humano sea capaz ni siquiera de recordarlo. Por ejemplo el hash SHA256 de la localización secreta de la siguiente megafiltración de WikiLeaks es: 66d9563648f3f23b2c90065a831e9357f2721-bd3965b95e1
e88a7e510c76026a.

Intente el lector entender semejante ristra.

El concepto filosófico más amplio que se utiliza aquí es el «Triángulo de Zooko». <<

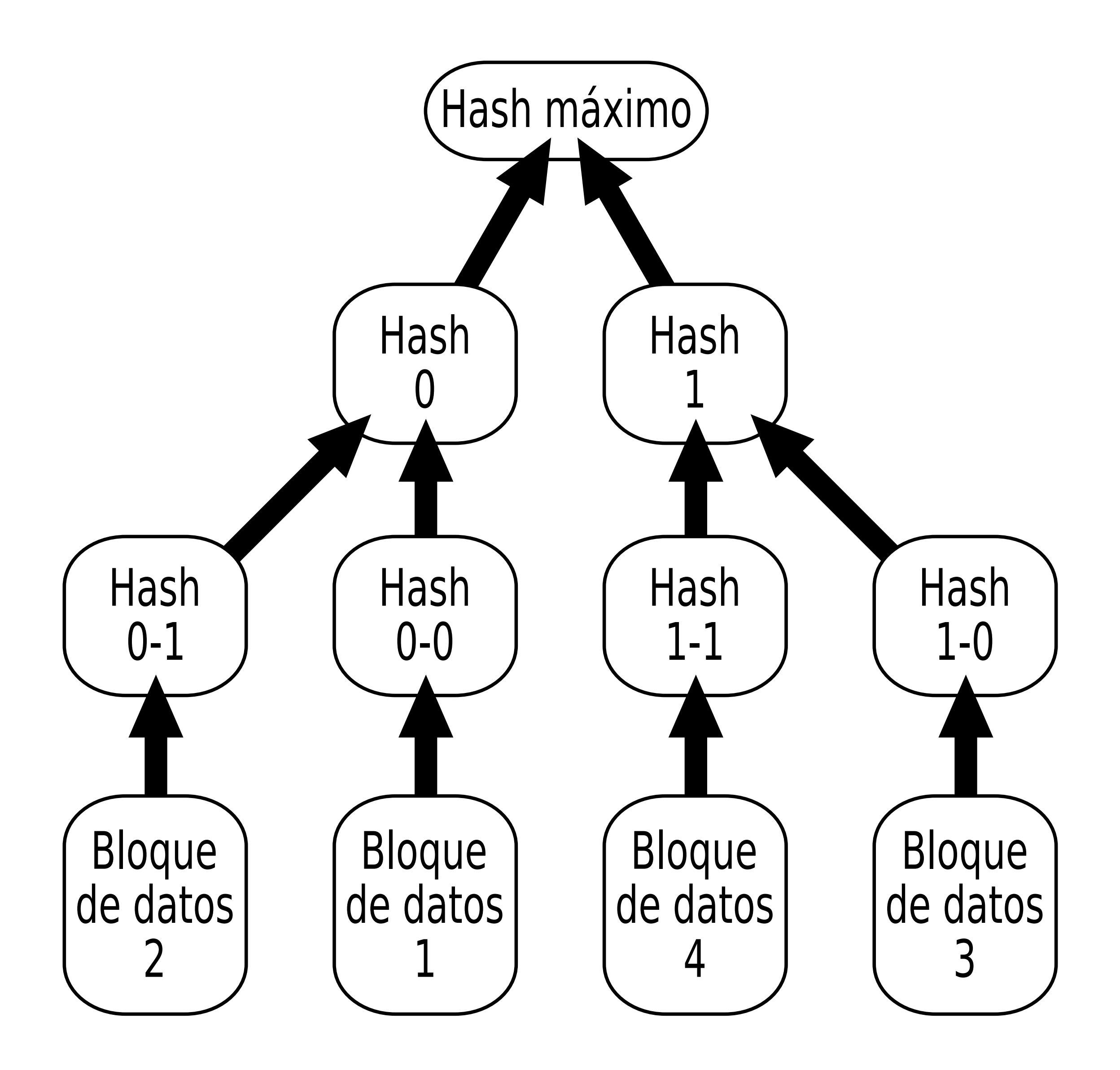
[176] En este contexto, «firmar» implica que el autor o editor de la información se sirve de un esquema de firma digital para crear una «firma» electrónica publicable que demuestra la autoría del hash. Ver «Public-Key Cryptography», *Wikipedia*, archive.today/2ue3r **<<**

[177] BitTorrent es un protocolo descentralizado de intercambio de archivos directamente entre usuarios. El desarrollo del protocolo de BitTorrent se ha visto impulsado por la necesidad de disponer de un método distribuido de intercambio que no tenga ningún punto débil. El «enlace magnético» es una extensión de este protocolo que proporciona una mayor resistencia a la censura.

Un enlace magnético es básicamente un hash seguro de un archivo (contiene otra información, pero en este caso no es relevante). En versiones avanzadas del protocolo BitTorrent se utiliza como «nombre de archivo» para encontrar copias del archivo solicitado, ubicadas en múltiples ordenadores poco fiables, sin necesidad de pasar por un directorio central. De esta forma, no existe ningún punto de ataque central que pueda usarse para censurar la distribución de archivos concretos.

Por todo ello, los enlaces magnéticos son un paso más en la evolución hacia la congruencia de los nombres de contenidos intelectuales. <<

[178] Un árbol hash es una estructura jerárquica compuesta de funciones hash de funciones hash



En este gráfico de un árbol hash, cada unidad situada sobre los bloques de datos contiene el hash de la información contenida en cada bloque. Así, Hash 0-0 contiene el hash del Bloque de Datos 1, Hash 0 contiene el hash de Hash 0-0 y Hash 0-1, y así sucesivamente. Ver «Merkle Tree», *Wikipedia*, archive.today/zfXgV

En un «árbol hash distribuido», las funciones hash que lo componen se distribuyen en muchos ordenadores. <<

[179] En otras palabras, se trata de utilizar un esquema de verificación digital en el que WikiLeaks publique una firma digital del hash como signo de que ese hash se corresponde con un documento que la propia WikiLeaks ha verificado y publicado, igual que el grabado de un editor en el interior de la cubierta de un libro, que es imposible de falsificar. <<

[180] El uso de un sistema de nombramiento como el propuesto, en el que el nombre es un hash basado en el contenido que representa, permite que si el contenido cambia lo más mínimo, el hash también cambia. Por ejemplo, el hash SHA256 del mensaje «Putin montó a caballo» es 1284ffaa16df7 c406c4528045e491f86cc3c57a9661a203aa-97914c19a09a0df. Pero si el mensaje se modifica, el hash cambia también. Por ejemplo, el hash SHA256 de «Putin montó a un caballo» es 9b24760c2ae1eba3cb8af2a8d75faa dd5cd4dcb492fdb31ce60caafa3eb8597e.

De forma similar, si el contenido es eliminado por completo, el hash no desaparece, como recordatorio de que el contenido existió y de que ha sido suprimido. <<

[181] El Bitcoin es un tipo de divisa digital codificada. Al igual que cualquier otra forma de dinero, puede ser intercambiada por dólares o por otras divisas, o utilizada para comprar productos, pero en su caso no existe un banco central que la almacene y gestione, y a diferencia de la dividas fiduciarias, no está controlada por un poder estatal.

El escrito al que se refiere es una entrada online del Foro de Bitcoin sobre el desarrollo del Namecoin, otra divisa similar derivada del concepto de Bitcoin: archive.today/aY5j0 <<

[182] «Los *cypherpunks* abogan por el uso de la criptografía y métodos similares como vía para lograr cambios sociales y políticos. Fundado a principios de los 90, el movimiento alcanzó sus momentos de máxima actividad durante las «criptoguerras» de dicha década y tras la primavera de Internet en 2011. El término cypherpunk, derivado de «cypher» (cifra/criptografía) y de «punk» fue añadido al *Oxford English Dictionary* en 2006». Ver Julian Assange con Jacob Appelbaum, Andy Müller-Maguhn, y Jérémie Zimmermann, *Cypherpunks: la libertad y el futuro de Internet* (Ediciones Deusto, 2013). <<

[183] A diferencia de la mayoría de las divisas, para las que existe un organismo financiero singular responsable de la impresión de todo el dinero, la fuente de los Bitcoins no es ningún ordenador individual. En lugar de eso, puesto que la unidad fundamental del Bitcoin se basa en la localización de funciones hash especiales, cualquier ordenador lo suficientemente potente puede «extraer de la mina» o producir Bitcoins. Para más información, ver la sección «Mining» en la parte de WikiLeaks dedicada a el Bitcoin: archive.today/LidYs <<

[184] Una colisión hash se produce cuando dos textos se codifican con el mismo hash. Por ejemplo, si nuestra función hash era «toma la primera letra de cada palabra», un ejemplo de colisión sería hash (Organización del Tratado del Atlántico Norte = OTAN = Obama Trata de Arreglar la Nación). Por definición, es imposible que un hash sea seguro si tiene una colisión, pero el Bitcoin utiliza un algoritmo llamado HashCash, por el cual las trabas para que no se produzca un problema de colisión se ajustan de tal forma que a medida que pasa el tiempo se hace cada vez más difícil que aparezcan, aunque no llega a ser imposible.

Los ordenadores conectados al sistema Bitcoin operan con cifras todo el día en busca de colisiones hash especiales, y cuando encuentran una se crea un Bitcoin. Este trabajo de computación requiere electricidad, por lo que la escasez de Bitcoins se deriva de la escasez de electricidad, creando un límite físico infranqueable a la velocidad a la que se pueden crear Bitcoins, de la misma forma que la energía requerida para extraer oro o plata de una mina crea escasez de estos metales, lo que evita inflaciones repentinas. <<

[185] El día en que tuvo lugar esta entrevista, el Bitcoin ya había superado al dólar y había alcanzado la paridad con el euro. A comienzos de 2014, su valor alcanzó los 1000 dólares, antes de caer hasta los 430 debido al despegue de otras criptodivisas derivadas del Bitcoin. Las inversiones estratégicas de WikiLeaks en Bitcoins nos proporcionaron un beneficio de más del 8000 por cien en tres años, lo que nos permitió eludir el bloqueo ilegal del sector bancario estadounidense. <<

[186] El término «clave pública» se deriva de la codificación de clave pública, también llamada codificación de clave asimétrica, un sistema criptográfico que se sirve de una combinación de dos claves diferentes: una privada y una pública. Ver «Criptografía asimétrica», *Wikipedia*, http://es.wikipedia.org/wiki/Criptografia_asimetrica

Un ejemplo de codificación de clave pública desarrollada para el correo electrónico es el programa criptográfico gratuito y de fuente abierta Pretty Good Privacy (*Privacidad bastante buena*, llamado PGP), creado inicialmente por Phil Zimmermann. Para más información, ver la página web de OpenPGP Alliance: **http://www.openpgp.org <<**

[187] Nuevamente se utiliza un objeto de la mesa como ejemplo. <<

[188] En otras palabras, si existen dos versiones de un mismo Bitcoin, ¿cómo se sabe cuál es la real y cual la copia? La respuesta está en el diseño. Bitcoin es una red entre usuarios iguales, sin autoridad central. El historial económico de los Bitcoins —qué Bitcoin pertenece a qué cuenta— se distribuye en ordenadores no relacionados y distribuidos por todo el mundo; de ahí el «problema de sincronización». Para solucionar esto, todos los ordenadores deben actualizar constantemente la información disponible para garantizar que todo el mundo tenga la misma visión sobre cada historial económico de los Bitcoins. De esta forma, se establece un consenso entre todos los dispositivos conectados a la red Bitcoin en cuanto a qué transacciones son válidas y cuáles no. <<

[189] Para hacerse una idea del valor de un nombre de domino corto, imagine el lector una dirección web llamada: **http://www.eldominiomaslargodelmundocondiferenciaymasymasymasymuchomas.com**, todo un infierno para el que no domine la mecanografía. <<

[190] En este contexto, «tupla» se refiere a una pareja «nombre, valor». Por ejemplo, (nombre, número de teléfono) o (nombre de dominio, dirección IP), o en este caso (nombre recordable por un humano, hash seguro). <<

[191] La frase «Primera Enmienda estadounidense» (tres palabras) representa el contenido de la Primera Enmienda a la Constitución de Estados Unidos, que establece que: «El Congreso no aprobará ley alguna que establezca oficialmente una religión, o que prohíba el libre ejercicio de una; o que coarte la libertad de expresión o de prensa; o el derecho de reunión pacífica o de petición al Gobierno de compensación por agravios».

Su hash SHA256 es 69be9b199c542c56183c408a23d7fd41fc878ec2634be6583db1659fb0e91063. <<

[192] En 2011, RSA Security, que ofrece servicios criptográficos a organismos gubernamentales, contratistas militares y bancos, sufrió un ataque informático y se sustrajeron un gran número de claves privadas. Poco después se informó de que las claves robadas estaban siendo utilizadas para entrar electrónicamente en otras compañías, como por ejemplo Lockheed Martin. <<

[193] En el momento de escribir este libro, esta sospecha está aún sin confirmar, aunque los archivos judiciales revelan que se dictaron órdenes secretas de subversión de las claves de codificado contra otras compañías estadounidenses. Ver el caso Lavabit: Megan Geuss, «Lavabit goes head-to-head with feds in contempt-of-court case», *Ars Technica*, 29 de enero de 2014, archive.today/zLrEs **<<**

[194] «Página de confianza» es un modelo de confianza descentralizado con PGP (el programa de codificación Pretty Good Privacy) que evita tener que depender de una autoridad central o jerárquica. Se trata de un modelo público basado en las relaciones de confianza entre usuarios que es imposible de falsificar, puesto que está provisto de una fuerte protección criptográfica. Pero esta criptografía también garantiza que las relaciones de confianza, una vez publicadas, no se puedan negar, puesto que no pueden ser falsificadas. Todo aquel que necesite realmente usar la criptografía no debería trabajar en la verificación y publicación criptográfica de sus relaciones de confianza con «co-conspiradores». <<

[195] «SSH» significa «Secure Shell» («*Intérprete de Órdenes Seguro*»). Es un protocolo utilizado para realizar una conexión codificada entre ordenadores. En particular SSH se puede usar como «controlador a distancia», un programa que te permite entrar en un ordenador desde otro y operar en él enviándole órdenes de comando. Los programas de control a distancia originales, como «RSH» o «telnet», utilizaban conexiones inseguras, por lo que sus atacantes podían subvertir la conexión. El SSH, inventado durante las criptoguerras de los años 90 por el programador finés Tatu Ylönen, utiliza por el contrario conexiones codificadas, que impiden tales ataques. La primera vez que un SSH se conecta a distancia a otro ordenador registra su clave pública, y desde ese momento cada vez que se vuelve a conectar coteja el ordenador con la clave original para asegurarse de que ningún atacante haya modificado la conexión. Por ello, si la primera conexión no es interceptada, ya no lo será ninguna de las siguientes. <<

[196] En los sistemas tradicionales de claves oportunistas como el SSH, la conexión inicial es la más vulnerable. Si un atacante te proporciona una clave falsa en esta primera conexión, podrá interferir en todas las conexiones subsiguientes sin ser detectado.

La idea en este caso es usar una «red inundada» para compartir claves, utilizando automáticamente las experiencias de los demás para crear un consenso sobre claves verdaderas, de forma que incluso durante la conexión inicial resulte fácil descubrir a un posible atacante. Esta idea puede verse en una variante de SSL llamada TACK (Trust Assertions for Certificate Keys), de Moxie Marlinspike. Ver **http://www.tack.io <<**

[197] El artículo referido es en realidad una publicación en Internet sobre el desarrollo de la Namecoin: archive.today/aY5j0

Para más información sobre las ideas subyacentes a la Namecoin, resulta indispensable leer la entrada «BitDNS and Generalizing Bitcoin» del Foro de Bitcoin: archive.today/9kEmz

También es interesante el fantástico y clarividente ensayo de Aaron Swartz sobre el «Triángulo de Zooko». Ver Aaron Swartz, «Squaring the Triangle: Secure, Decentralized, Human-Readable Names», aaronsw.com, archive.today/pIvtj <<

[198] «In Conversation with Julian Assange Part I», WikiLeaks, 23 de mayo de 2011, archive.today/E9IOb <<

[199] Este proveedor era Noor Group, que en realidad poseía un 8 % del mercado. <<

[200] La idea básica se llama «red de malla». Cada teléfono transmite sus comunicaciones a través de otros teléfonos ubicados dentro de su campo de cobertura, en lugar de tener que hacerlo a través de las antenas y redes de las compañías telefónicas. <<

[201] «GSM» significa «Global System for Mobile Communications» y es el principal sistema de telecomunicación de telefonía móvil del mundo. Un teléfono GSM es simplemente un teléfono móvil corriente. <<

[202] Las torres propiedad de las compañías de telefonía móvil. <<

[203] Por ejemplo, para lograr economías de escala, los fabricantes de teléfonos móviles se han preocupado de crear terminales que funcionen en la mayoría de los países. Esto significa que deben ser compatibles con las diversas frecuencias y estándares de codificación utilizadas en cada país, de la misma forma que un transformador universal de corriente tiene clavijas adaptables a los diferentes tipos de enchufe existentes en cada país. <<

[204] WiMAX es el estándar Worldwide Interoperability for Microwave Access (Interoperabilidad Global para el Acceso por Microondas), un tipo de patrón criptográfico de comunicación de datos sin cables que a menudo funciona a distancias muy superiores a las disponibles actualmente. <<

[205] Ver OpenBTS: **http://www.openbts.org <<**

[206] Un reciente ejemplo de esto ocurrió en 2011 en San Francisco. Con el fin de impedir la celebración de #OpBART, una protesta planificada contra una serie de ataques letales del cuerpo de policía de la red de transportes Bay Area Rapid Transit, las autoridades dejaron sin servicio a un cierto número de estaciones emisoras a lo largo de dicha red. <<

[207] En este contexto, un túnel es un canal de comunicación entre dos puntos utilizando para ello a un tercero. <<

[208] «UDP» significa «User Datagram Protocol», un protocolo simple y rápido para enviar paquetes individuales de información de un servidor de Internet a otro. <<

[209] Esto es, escogiendo direcciones de Internet de forma aleatoria. <<

[210] La mayoría de los usuarios de Internet se protegen tras un cortafuegos o cualquier otro mecanismo (como «Network Address Trasnlation», más conocido como NAT) que bloquea la recepción de conexiones iniciadas por otra parte. Cuando dos usuarios desean comunicarse entre ellos directamente, sencillamente no pueden. La perforación es una técnica que engaña a los cortafuegos o NAT para que establezcan comunicación directa, en lugar de tener que transmitir la comunicación a través de un servidor, que puede no ser de fiar. <<

[211] En este contexto, «servidor» alude a un ordenador conectado a Internet que puede aceptar conexiones entrantes. <<

[212] El ancho de banda es pequeño porque los datos enviados son mínimos: concretamente, están compuestos de texto codificado en un paquete UDP. <<

[213] Una «aplicación asesina» (en inglés, *killer application*, o simplemente *killer app*) es un programa informático tan útil o tan popular que por sí mismo hace que merezca la pena disponer de todo aquello con lo que esté asociado. <<

[214] Esto es, no limitado a un UDP, lo que implica que las personas que utilicen diferentes tipos de conexiones podrán comunicarse. <<

[215] «TCP» o «Transmission Control Protocol» es el protocolo de Internet más común. Más complejo que el UDP, se utiliza por ejemplo para comunicar la mayor parte del contenido de las páginas web. <<

[216] Es decir, el problema no se debe a una capacidad limitada de comunicación electrónica. <<

[217] En este contexto, «una tubería» significa un enlace de telecomunicación internacional, que es todo cuanto se necesita para que la información salga desde el interior de un país a una red más amplia. <<

[218] En jerga tecnológica, «proyectar» significa «diseñar». <<

[219] El político conservador y autoritario Antonio de Oliveira Salazar fue el primer ministro y dictador *de facto* de Portugal entre 1932 y 1968. El gobierno llamado «Estado Novo» instaurado por él le sobrevivió hasta 1974, año en el que fue derrocado por un golpe militar izquierdista y se restauró la democracia.

Tras un golpe de estado en 1967, Grecia pasó a estar gobernada por una junta militar apoyada por Estados Unidos y conocida como el «Junta de los Coroneles», que también fue derrocada por un alzamiento democrático en 1974.

Este fue un momento muy importante para el sur de Europa. El dictador español, Francisco Franco, murió solo un año después, en 1975, entregando el poder al rey Juan Carlos I, quien facilitó la restauración de la democracia española.

La publicación de WikiLeaks basada en los telegramas de Kissinger, trata en profundidad este periodo. Ver **http://www.wikileaks.org/plusd <<**

[220] En 1991, cuando Phil Zimmermann lanzó el PGP, los programas de criptografía fueron calificados material restringido por la ley federal de Estados Unidos, por lo que no podían ser exportados. Como el PGP estaba colgado en Internet y alguien externo a Estados Unidos había descargado el programa, se consideró a Zimmermann culpable de exportación, por lo que estuvo bajo la investigación de un gran jurado federal estadounidense durante tres años. Durante los años 90, la ASN y el FBI orquestaron una campaña para intentar detener la propagación de la criptografía, campaña que pasó a conocerse como «criptoguerra» (para más información, ver nota al pie 236). Cuando prescribió el delito por el que se le acusaba, Zimmermann admitiría que había subido deliberadamente el sistema PGP a Internet para intentar difundir la criptografía antes de que fuese prohibida. <<

[221] *El señor de las moscas* es una novela de William Golding sobre un grupo de colegiales atrapados en una isla desierta que, a medida que se van rompiendo las restricciones sociales, van descubriendo el lado más oscuro de la naturaleza humana. William Golding, *El señor de las moscas* (Alianza Editorial, 2003) <<

[222] «Protein synthesis: an epic on the cellular level», Departamento de Química de la Universidad de Stanford, 1971. Disponible en YouTube en youtu.be/u9dhO0iCLww <<

[223] Dependiendo de cómo se manejen las cifras, el punto más alto del salario medio masculino se alcanzó entre mediados y finales de los años 70. Ver página 50 de Carmen DeNavas-Walt, Bernadette D. Proctor, y Jessica C. Smith, «Income, Poverty, and Health Insurance Coverage in the United States: 2012», Departamento de Comercio de Estados Unidos, Administración de Economía y Estadística, Oficina Censal de Estados Unidos, septiembre de 2013, is.gd/xJ9wPV <<

[224] «IRS» significa «Internal Revenue Service» («*Servicio de Ingresos Nacionales*»), y es el organismo público encargado de la recaudación de impuestos para el gobierno estadounidense. Es el equivalente a la Agencia Tributaria española. <<

[225] Un grupo de ordenadores conectados por Internet en el que cada ordenador únicamente conoce una cantidad limitada de las direcciones de los demás participantes. Una red oscura es difícil de censurar, pero también es comparativamente difícil de acceder. I2P es un ejemplo de red oscura: **http://www.i2p2.de <<**

[226] «FOI» alude a una petición de «freedom of information» (libertad de información), una petición de la información legalmente disponible sobre un organismo público, en países con leyes que defienden la libertad de información. <<

[227] «UK Ministry of Defence continually monitors WikiLeaks: eight reports into classified UK leaks, 29 Sep 2009», WikiLeaks, 30 de septiembre de 2009, archive.today/6pMbw <<

[228] BT, antiguamente British Telecom, es la empresa de telecomunicaciones más grande de Reino Unido, y una de las más grandes del mundo. <<

[229] Greg Mitchell, *So Wrong for So Long: How the Press, the Pundits —and the President— Failed on Iraq* (Union Square Press, 2008). <<

[230] Para una discusión más profunda sobre esta idea, ver Raffi Khatchadourian, «No Secrets: Julian Assange’s mission for total transparency», *The New Yorker*, 7 de junio de 2010, archive.today/zZYqJ <<

[231] Geoffrey Miller es el general del ejército de Estados Unidos que estuvo al mando simultáneamente de las instalaciones de la bahía de Guantánamo, Cuba, y de Abu Ghraib, en Irak.

Donald Rumsfeld fue el secretario de Defensa de Estados Unidos entre 2001 y 2006 (y anteriormente entre 1975 y 1977). <<

[232] «Camp Delta Standard Operating Procedure», WikiLeaks, 7 de noviembre de 2007, archive.today/P9HMH

Ver también Julian Assange, Daniel Mathews, con Emi Maclean, Marc Falkoff, Rebecca Dick, y Beth Gilson (consejeros), «Changes in Guantanamo Bay SOP manual (2003–2004)», WikiLeaks, 3 de diciembre de 2007, archive.today/b3A1g <<

[233] La «mina» se refiere en este caso al lugar más cercano al trabajo obrero de base. <<

[234] La Conferencia de Wannsee fue una reunión de altos mandos nazis en la que se coordinó la implementación de la «Solución Final», en la que millones de judíos residentes en la Europa dominada por los nazis fueron exterminados en campos de concentración. <<

[235] La frase «banalidad del mal» procede del libro *Eichmann en Jerusalén: un informe sobre la banalidad del mal* de la filósofa Hannah Arendt. Esta frase ha pasado a designar aquella banalidad irreflexiva que a menudo se ve en la deshumanización sistematizada, que parece surgir de la abstracción, la falsedad, la adaptación u otros procesos de normalización. <<

[236] Esto es una referencia a la «criptoguerra» de los años 90. Cuando los activistas del movimiento cypherpunk comenzaron a difundir buenas herramientas criptográficas como *software* gratuito, la administración de Estados Unidos tomó medidas para evitar que estas herramientas se utilizasen de forma efectiva: las clasificó como material restringido para la exportación; intentó introducir tecnologías rivales deliberadamente defectuosas, de forma que la policía y las agencias de inteligencia siempre pudieran descifrar la información; y también intentó implantar el controvertido «depósito de claves». Durante un corto periodo tras el cambio de siglo, la impresión general fue que estos esfuerzos habían sido derrotados. Sin embargo, actualmente está teniendo lugar una «segunda criptoguerra», en la que se están realizando nuevos intentos legislativos, técnicos y encubiertos para crear puertas traseras o para marginar el uso de la criptografía. <<

[237] *Daño Colateral* es un vídeo publicado por WikiLeaks que muestra las imágenes de un helicóptero militar estadounidense matando indiscriminadamente civiles en Irak, incluyendo a dos periodistas de Reuters. En el momento de escribir estas líneas ya ha superado los 14 millones de visitas en YouTube. «Collateral Murder — WikiLeaks — Iraq» (vídeo), subido a la red el 3 de abril de 2010, youtu.be/5rXPrfnU3G0. Existe una versión subtitulada al español en youtube.com/watch?v=teCB48QT1zs <<

[238] La cifra ofrecida en julio de 2010 fue de 854 000 personas. Ver Dana Priest, William M. Arkin, «A hidden world, growing beyond control», *The Washington Post*, 19 de julio de 2010, archive.today/3C0wq

En 2014 esta cifra ha aumentado hasta el millón y medio. Ver Brian Fung, «5.1 million Americans have security clearances. That’s more than the entire population of Norway», *The Washington Post*, 24 de marzo de 2014, archive.today/46So6 **<<**

[239] En el momento de esta conversación (2011), la cifra más aceptada era 2,5 millones, cifra procedente de un informe de la Oficina de Responsabilidad Financiera del Gobierno, elaborado en 2009. Ver Steven Aftergood, «More Than 2.4 Million Hold Security Clearances», *Secrecy News*, 29 de julio de 2009, archive.today/kThm8

Sin embargo, en septiembre de 2011 aparecieron nuevos estudios que elevaron la cifra hasta los 4,2 millones. Ver Steven Aftergood, «Number of Security Clearances Soars», Secrecy News, 20 de septiembre de 2011, archive.today/Hw6x2

En 2014 la cifra asciende ya hasta los 5,1 millones, un estado dentro de un estado, con una población mayor que la de Noruega. Ver Brian Fung, «5.1 million Americans have security clearances. That's more than the entire population of Norway», *The Washington Post*, 24 de marzo de 2014, archive.today/46So6 <<

[240] Por ejemplo, *The New York Times* se jactó de que la Casa Blanca les había agradecido que manejasen «la documentación con cuidado». «The War Logs Articles», *The New York Times*, 25 de julio de 2010, archive.today/a2lVO <<

[241] *Amnesty International Report 2011: The state of the world's human rights* (informe), Amnistía Internacional, mayo de 2011, pp. xiv–xvi, is.gd/C4JNVP

Ver también «WikiLeaks: The secret life of a superpower» Episodio 1 (documental), BBC, primera emisión 21 de marzo de 2012, archive.today/pKuQZ. En vez de transcripción, hay subtítulos disponibles de Amara: archive.today/uak1V

Ver también «Deconstructing Tunileaks: An Interview with Professor Rob Prince, University of Denver», *Nawaat*, 20 de diciembre de 2010, archive.today/5TiD4

Ver también Lina Ben Mhenni, «Tunisia: Censorship Continues as WikiLeaks Cables Make the Rounds», *Global Voices Advocacy*, 7 de diciembre de 2010, archive.today/MW9aR <<

[242] «The looting of Kenya under President Moi», WikiLeaks, 30 de agosto de 2007, actualizado el 9 de septiembre de 2007, archive.today/JdHZ4

Ver también «Kenyan Presidential Election, 2007», *Wikipedia*, archive.today/TEj60

Ver también «2007–08 Kenyan Crisis», *Wikipedia*, archive.today/Rgg1g

Ver también «Corruption in Kenya», *Wikipedia*, archive.today/b7ve8

Ver también Xan Rice, «The looting of Kenya», *The Guardian*, 31 de agosto de 2007, archive.today/VR7V1

Ver también Nick Wadhams, «Kenyan President Moi's 'corruption' laid bare», *The Telegraph*, 1 de septiembre de 2007, archive.today/KxkB1

Ver también Barney Jopson, «Kenya graft in spotlight», *Financial Times*, 31 de agosto de 2007, archive.today/k2t0i <<

[243] WikiLeaks ha promovido la existencia de un entorno editorial libre desde su creación. Además de practicar ellos mismos la libertad de expresión, sus contribuciones más notables han sido la publicación de las listas negras de censura en Internet, y su papel como asesor de la Iniciativa Islandesa para Medios de Comunicación Modernos. Ver «Internet Censorship», WikiLeaks, archive.today/EfZ6g

Ver también Julian Assange, «WikiLeaks editor: why I'm excited about Iceland's plans for journalism», *The Guardian*, 15 de febrero de 2010, archive.today/lK3u2

Ver también Chris Vallance, «WikiLeaks and Iceland MPs propose 'journalism haven'», BBC, 12 de febrero de 2010, archive.today/cOjgM

Ver también la página del International Modern Media Institute: **http://www.immi.is <<**

[244] El Banco Julius Baer (BJB) era el grupo bancario privado más grande de Suiza. En 2008. WikiLeaks publicó unos documentos que revelaban una masiva evasión fiscal cometida por individuos y corporaciones asociadas con BJB, con cuentas ocultas en las Islas Caimán. El grupo bancario respondió con una imputación judicial sobre Dynadot, el registro público californiano del nombre de dominio WikiLeaks. Esto provocó la indignación pública, y la imputación fue revocada cuando una coalición de editores, entre los que estaba Associated Press, presentó al tribunal un *amicus curiae*. Al final, BJB desistió de presentar cargos. Ver Bank Julius Baer & Co. Ltd. Et al v. WikiLeaks et al, JUSTIA Dockets & Filings, archive.today/BEaNB

Ver también «Full correspondence between WikiLeaks and Bank Julius Baer», WikiLeaks, 19 de febrero de 2008, archive.today/3k3Lf

Ver también Kim Zetter, «Cayman Islands Bank Gets WikiLeaks Taken Offline in U.S. — Updated with Links». *Wired*, 18 de febrero de 2008, archive.today/vND8k <<

[245] Poco después de su intento fallido de censura contra WikiLeaks, el Banco Julius Baer canceló su oferta pública inicial de acciones en Estados Unidos. Ver Securities and Exchange Commission, Form S-1, Julius Baer Americas Inc., 6282 (Primary Standard Industrial Classification Code Number), archive.today/WaUt1

Ver también Christopher Condon, «Baer to Sell Up to $1 Billion in U.S. Fund Unit (Update3)», *Bloomberg*, 12 de febrero de 2008, archive.today/cowj2

Ver también Richard Koman, «Bank that censored WikiLeaks was preparing for IPO», *ZDNet*, 20 de febrero de 2008, archive.today/r2rur <<

[246] Ver la transcripción de la rueda de prensa: «DOD News Briefing with Geoff Morrell from the Pentagon» (transcripción), Departamento de Defensa de Estados Unidos, 5 de agosto de 2010, archive.today/nHyaW

La rueda de prensa también se puede ver en YouTube: «Pentagon Press Conference re: WikiLeaks Part 1 of 4» (vídeo), subida el 26 de septiembre de 2010, youtu.be/DJe_Q8XFIHI <<

[247] *The Iraq War Diaries*, WikiLeaks, 22 de octubre de 2010, warlogs.wikileaks.org <<

[248] El club al que se refiere es el Frontline Club, una popular asociación de reporteros y periodistas de guerra ubicada en el área londinense de Paddington. Este club ha acogido algunas de las ruedas de prensa más importantes de WikiLeaks. **http://www.frontlineclub.com** **<<**

[249] En 1994, durante aproximadamente 100 días, los hutus exterminaron entre 500 000 y 1 millón de tutsis, aproximadamente el 20 % de la población del país. <<

[250] Por ejemplo, ver «Assorted plans and papers from the Iranian Ammunition Industries Group, 2009», WikiLeaks, 17 de julio de 2009, archive.today/Ycl1m

Ver también Julian Assange, «Serious nuclear accident de mayo de lay behind Iranian nuke chief’s mystery resignation», WikiLeaks, 17 de julio de 2009, archive.today/wCbof <<

[251] Las publicaciones de WikiLeaks pueden buscarse por países en

Para ejemplos de países africanos, ver WikiLeaks: archive.today/reC33

Para ejemplos de Timor Oriental, ver WikiLeaks: archive.today/vQtYO **http://www.wikileaks.org/wiki/Category:Countries <<**

[252] RuLeaks: **http://www.ruleaks.net** <<

[253] El SFS es el Servicio Federal de Seguridad de la Federación Rusa, el sucesor de la KGB. <<

[254] Las primeras publicaciones de WikiLeaks, en 2006, trataban sobre Somalia, concretamente sobre la Unión Somalí de Tribunales Islámicos. Algunos de los documentos recibidos procedían de China. Ver WikiLeaks: archive.today/ewGbU

Ver también «Inside Somalia and the Union of Islamic Courts», WikiLeaks, archive.today/emqVb **<<**

[255] Ver lista de publicaciones de WikiLeaks para el año 2007: archive.today/zER02 <<

[256] La cifra en Estados Unidos era realmente del 81 %, según un estudio de Ipsos llevado a cabo en abril de 2011. El porcentaje global era del 79 % y de hasta el 92 % en Australia. Ver «Ipsos Global @dvisory: Julian Assange and WikiLeaks», Ipsos, 26 de abril de 2011, archive.today/BnV1S <<

[257] Entre 1983 y 1997, Eric Schmidt trabajó en Sun Microsystems, Inc., donde, como director jefe de las áreas tecnológica y corporativa, lideró el desarrollo del proyecto de creación del lenguaje de programación Java. <<

[258] Antes de ser contratado por Larry Page y Sergey Brin para ponerse al timón de Google en 2002, Eric Schmidt era presidente y consejero delegado de Novell. <<

[259] Pueden verse algunos ejemplos en la página web de cabledrum:

Las páginas cables.mrkva.eu y cablegatesearch.net proporcionan excelentes comparaciones entre textos censurados y textos originales, con el fin de comprobar las censuras que realizan os medios de comunicación vinculados con WikiLeaks. **http://www.cabledrum.net/pages/censorship.php <<**

[260] En este ejemplo, el documento original contenía 5226 palabras, y la versión censurada de *The Guardian* tenía solo 1406 palabras. El documento original puede verse en Identificación canónica: 05SOFIA1207_a, Biblioteca Pública de la Diplomacia de Estados Unidos, WikiLeaks, archive.today/ryqvN

Para la versión censurada, ver «US embassy cables: Organised crime in Bulgaria», *The Guardian*, 1 de diciembre de 2010, archive.today/faYa6

Para el artículo de *The Guardian* basado en el documento, ver «WikiLeaks cables: Russian government 'using mafia for its dirty work'», *The Guardian*, 1 de diciembre de 2010, archive.today/WYKEe

El alcance de la censura puede verse en la página web de Cablegatesearch, que muestra las modificaciones destacadas en rosa: archive.today/rdVYl

Este ejemplo relativo a Bulgaria aparece en el socio de comunicación búlgaro de WikiLeaks *Bivol*, en «Unedited cable from Sofia shows the total invasion of the state by organized crime (Actualización: Comparación de Documentos», *WL Central*, 18 de marzo de 2011, archive.today/kmvLt

Además, ver «The Guardian: Redacting, censoring or lying?», *WL Central*, 19 de marzo de 2012, archive.today/YR3VN

También es de destacar el comentario del periodista de *The Guardian* David Leigh y todas las respuestas sobre ambos artículos del *WL Central*. <<

[261] El documento original puede verse en Identificación canónica: 10ASTANA72_a, Biblioteca Pública de la Diplomacia de Estados Unidos, WikiLeaks, archive.today/VSyHl

Para la versión censurada de *The Guardian*, ver «US embassy cables: Kazakhstan — the big four», *The Guardian*, 29 de noviembre de 2010, archive.today/O08ut

El alcance de la censura puede verse en la página web de Cablegatesearch, que muestra las modificaciones destacadas en rosa: archive.today/Nm1k4 <<

[262] Un documental coproducido por WikiLeaks y Sixteen Films, llamado *Mediastán* (2013), incluyó una entrevista con el editor de *The Guardian*, Alan Rusbridger, en el que Rusbridger explica las razones de la autocensura del periódico. Este segmento está disponible en YouTube: «Mediastan: The Rushbridger [*sic*] extract» (vídeo), subido el 11 de octubre de 2013, youtu.be/ZNgFDFibit0 <<

[263] Para una mayor profundización en este punto con más ejemplos concretos, ver Julian Assange con Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann, *Cypherpunks: la libertad y el futuro de Internet* (Ediciones Deusto, 2013). <<

[264] Un vídeo de YouTube puede insertarse en una página web, de forma que puede verse directamente en dicha página sin tener que ir a YouTube. **<<**

[265] YouTube es propiedad de Google. <<

[266] «Massive Takedown of Anti-Scientology vídeos on YouTube», Electronic Frontier Foundation, 5 de septiembre de 2008, archive.today/fQ1Do <<

[267] «IA» es la abreviatura de «inteligencia artificial». <<

[268] Un fraude de «inflar y tirar» es un típico fraude del mercado bursátil, en el que el estafador compra acciones de empresas de baja liquidez e inmediatamente «infla» las acciones difundiendo rumores de que el precio está a punto de subir. Si tiene éxito, mucha gente comprará las acciones antes de que se produzca esa supuesta subida, con el resultado de que el aumento de demanda provoca en sí mismo una subida de los precios, momento en el que el estafador se apresura a «tirar» sus acciones, vendiéndolas con beneficio al precio inflado, antes de que dicho precio caiga y vuelva a la normalidad. <<

[269] «OCR» son las siglas de «optical character recognition» («*reconocimiento óptico de caracteres*»), una forma de traducir imágenes de texto (por ejemplo, textos escaneados) a caracteres que un ordenador pueda reconocer.

La aparición del correo electrónico, y con ello la del «spam» o correo basura, proporcionó a los estafadores nuevas formas de «inflado». Con el fin de esquivar los filtros antispam que controlan palabras clave relacionadas con la jerga bursátil, estos estafadores empezaron a enviar su *spam* en forma de archivos de imagen GIF, diseñados para ser indetectables por los ordenadores con tecnología OCR, pero perfectamente legibles por las pretendidas víctimas. <<

[270] Para más información sobre el incidente de HBGary, ver el epígrafe «Trasfondo de EE. UU. contra WikiLeaks». <<

[271] Una investigación de Associated Press reveló que entre 2004 y 2009 el dinero gastado por el Ejército de Estados Unidos para «ganarse los corazones y las mentes» aumentó un 63 %, hasta alcanzar una cifra de 4700 millones de dólares. Durante ese periodo, la sección de relaciones públicas, publicidad y recursos humanos del Departamento de Defensa, con sus 27 000 empleados, era casi tan grande como toda la fuerza de trabajo del Departamento de Estado al completo. Durante el último año, un único proyecto intentó introducir más de 10 000 elementos de relaciones públicas en los medios de comunicación, incluyendo 5400 comunicados de prensa, 3000 anuncios en televisión y 1600 entrevistas. Ver «Pentagon Spending Billions on PR to Sway World Opinion», Fox News, 5 de febrero de 2009, archive.today/30Npv <<

[272] «MOU between Raila Odinga and Muslims», WikiLeaks, 14 de noviembre de 2007, archive.today/giXkU <<

[273] Referencia a la discusión previa sobre la cultura en la Universidad de Stanford en 1971. <<

[274] «TEF» son las siglas de «transferencia electrónica de fondos» <<

[275] Para más información sobre esto, ver «Trasfondo de EE. UU. contra WikiLeaks». <<

[276] Para más información sobre el «caso de la citación de Twitter», ver Trasfondo de EE. UU. contra WikiLeaks». **<<**

[277] En este ejemplo concreto, «una FISA» es la abreviación de «una petición FISA», es decir, una petición legal de registros electrónicos conforme a la FISA. «FISA» son las siglas de «Foreign Intelligence Surveillance Act» (Ley de Vigilancia de la Inteligencia Extranjera), una ley de Estados Unidos que autoriza la vigilancia física y electrónica, actualmente muy conocida en todo el mundo tras las filtraciones de Edward Snowden sobre la FISA y sus operaciones judiciales. Para más información sobre la FISA, ver «Surveillance Under the Foreign Intelligence Surveillance Act (FISA)», Electronic Frontier Foundation, archive.today/ibU4C <<

[278] Para más información sobre esto, ver «Trasfondo de EE. UU. contra WikiLeaks». <<

[279] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), pp. 39–40. <<

[280] Ibid., p. 41. <<

[281] Ibid., p. 163. <<

[282] Ibid., nota 3, capítulo 5, p. 163. <<

[283] Ibid., p. 42. <<

[284] Ed Pilkington, «Bradley Manning leak did not result in deaths by enemy forces, court hears», *The Guardian*, 31 de julio de 2013, archive.today/lYznz
<<

[285] Adam Levine, «Gates: Leaked documents don’t reveal key intel, but risks remain», CNN, 17 de octubre de 2010, archive.today/HzJxM <<

[286] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 42. <<

[287] Ibid., p. 44. <<

[288] Ibid., pp. 42 y 44. <<

[289] Ibid., p. 45. <<

[290] Ibid., p. 47. <<

[291] John Hudson, «Eric Schmidt: Money is the only reason Julian Assange redacted WikiLeaks files», *Foreign Policy*, 19 de abril de 2013, archive.today/UGU5E <<

[292] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 47. <<

[293] Ibid., nota 111, en referencia a la p. 110: «Contacto con telecomunicaciones chinas: cablegrama de WikiLeaks, ‘Motivo: potencial sofocado: un cablegrama por fibra óptica llega a Tanzania, Origen: Embajada Dar Es Salaam (Tanzania), hora del cable: Vie. 4 Sep. 2009 04:48 UTC’, **http://www.cablegatesearch.net/cable.php?id=09DARESSALAAM585»**
<<

[294] Juzgados conforme a la misma ley que llevó a la muerte al activista Aaron Swartz, la «Computer Fraud and Abuse Act» («*Ley de Fraude y Abuso Informático*»), o CFAA. <<

[295] Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013), p. 163. <<

[296] Ibid., p. 165. <<

[297] Ibid., «Afterword for the Paperback Edition». <<

[298] Ver el apartado «La banalidad del ‘No seas malo’» <<

[299] «Cómplices» es como el general James Clapper, director de la Inteligencia Nacional de Estados Unidos, llamó a todos aquellos que habían ayudado a Edward Snowden. Ver DS Wright, «General Clapper Labels Journalists Snowden's 'Accomplices'», *FireDogLake*, 30 de enero de 2014, archive.today/91i07 <<

[300] En lugar de, por ejemplo, destacar la «ironía» de que Estados Unidos no sea un lugar seguro para ejercer el derecho a la libre expresión recogido en la Primera Enmienda de su propia Constitución, o la «ironía» de que Europa haya estado tan preocupada por su relación geopolítica con Estados Unidos que ninguna nación europea, con la excepción de Rusia, haya aceptado las peticiones de asilo de Snowden. **<<**

[301] «Afterword for the Paperback Edition» en Eric Schmidt y Jared Cohen, *The New Digital Age*, edición británica en tapa blanda (John Murray, 2013). <<

[302] Ewen MacAskill, «NSA paid millions to cover Prism compliance costs for tech companies», *The Guardian*, 23 de agosto de 2013, archive.today/wNBZE <<

[302] *Daño Colateral*: **http://www.collateralmurder.com**

Diarios de la guerra de Irak: **http://www.wikileaks.org/irq**

Diarios de la guerra de Afganistán: **http://www.wikileaks.org/afg**

Cablegate: **http://www.wikileaks.org/cablegate.html <<**

[304] «Congressional committee holds hearing on national security leak prevention and punishment», Comité de reporteros por la libertad de prensa, 11 de julio de 2012, archive.today/NAHgG <<

[305] Affidávit de Julian Paul Assange, WikiLeaks, 2 de septiembre de 2013, archive.today/doiGA#3 <<

[306] Affidávit de Julian Paul Assange, WikiLeaks, 2 de septiembre de 2013, archive.today/0gUpy#5 <<

[307] Raphael Satter, «Minister: Iceland refused to help FBI on WikiLeaks», Associated Press, 1 de febrero de 2013, archive.today/Fgtyw <<

[308] Peter Stanners, «FBI met WikiLeaks informant in Copenhagen», *The Copenhagen Post*, 15 de agosto de 2013, archive.today/b2bL0 <<

[309] «Iceland Minister: FBI Used Hacker to Bait WikiLeaks», *Iceland Review*, 14 de febrero de 2013, actualizado el 30 de enero de 2014, archive.today/ZXsvF <<

[310] «US Military refers to Julian Assange and WikiLeaks as the ‘enemy’ with the ‘victims’ being ‘society’», WikiLeaks, 26 de septiembre de 2012, actualizado el 27 de septiembre de 2012, archive.today/vOZv5 <<

[311] «Judge in WikiLeaks FOIA Cites ‘Events that Have Transpired,’ Government Claims FOIA Is ‘Improper’», *emptywheel*, 10 de abril de 2014, archive.today/QVpR7

Esto fue confirmado en mayo de 2014. Ver Philip Dorling, «Assange targeted by FBI probe, US court documents reveal», *Sydney Morning Herald*, 20 de mayo de 2014, archive.today/zFhv7

Para los documentos mencionados en el artículo del *Sydney Morning Herald*, ver Case 1:12-cv-00127-BJR en el Tribunal de Distritos de Estados Unidos para el Distrito de Columbia: is.gd/hvvmgM <<

[312] Glenn Greenwald, «WikiLeaks Grand Jury investigation widens», *Salon*, 9 de junio de 2011, archive.today/SH0O9 <<

[313] «Part 2: Daniel Ellsberg and Jacob Appelbaum on the NDAA, WikiLeaks and Unconstitutional Surveillance», *Democracy Now!*, 6 de febrero de 2013, archive.today/gHd46

Ver también Elinor Mills, «Researcher detained at U.S. border, questioned about WikiLeaks», *CNET*, 1 de agosto de 2010, archive.today/iCiPL

Ver también Xeni Jardin, «WikiLeaks volunteer detained and searched (again) by US agents», *Boing Boing*, 12 de enero de 2011, archive.today/1LtnW

Ver también Paul Fontaine, «Jacob Appelbaum Detained At Keflavík Airport», *Reykjavík Grapevine*, 27 de octubre de 2011, archive.today/4AJlF

Ver también «Snowden ally Appelbaum claims his Berlin apartment was invaded», *Deutsche Welle*, 21 de diciembre de 2013, archive.today/gvdlh

Ver también Andrew Fowler, Wayne Harley, «Sex, Lies and Julian Assange» (vídeo), *Four Corners*, ABC, 23 de julio de 2012, actualizado el 16 de mayo de 2013, archive.today/HCpDj <<

[314] Alexa O'Brien, «WikiLeaks Grand Jury | 7 civilians being target by FBI for #WLGrandJury including #WikiLeaks founders, associates», alexaobrien.com, 21 de junio de 2012, archive.today/cJ0Ho <<

[315] Ed Pilkington, «Bradley Manning’s treatment was cruel and inhuman, UN torture chief rules», *The Guardian*, 12 de marzo de 2012, archive.today/DRcZq <<

[316] Kim Zetter, «Bradley Manning Charged With 22 New Counts, Including Capital Offense», *Wired*, 3 de febrero de 2011, archive.today/X6Y4A <<

[317] Ed Pilkington, «Bradley Manning denied chance to make whistleblower defence», *The Guardian*, 17 de enero de 2013, archive.today/Kn8EQ **<<**

[318] Alexa O'Brien, «Pfc. Manning's Statement for the Providence Inquiry», alexaobrien.com, 28 de febrero de 2013, archive.today/Fjjo0 **<<**

[319] Tom McCarthy, «Bradley Manning tells lawyer after sentencing: ‘I’m going to be OK’ — as it happened», *The Guardian*, 21 de agosto de 2013, archive.today/kND5Y <<

[320] «Chelsea Manning’s 35-year prison sentence upheld by US army general», *The Guardian*, 14 de abril de 2014, archive.today/GP08a <<

[321] Nick Collins, «WikiLeaks: guilty parties ‘should face death penalty ’»,*The Telegraph*, 1 de diciembre de 2010, archive.today/RG81n <<

[322] «DOD News Briefing with Geoff Morrell from the Pentagon» (transcripción), página web del Departamento de Defensa de Estados Unidos, 5 de agosto de 2010, archive.today/F3CC1

Ver también Philip Shenon, «The General Gunning for WikiLeaks», *The Daily Beast*, 9 de diciembre de 2010, archive.today/xx5gK <<

[323] Philip Shenon, «U.S. Urges Allies to Crack Down on WikiLeaks», *The Daily Beast*, 8 de octubre de 2010, archive.today/Dvkgy **<<**

[324] Charles Arthur, Josh Halliday, «WikiLeaks fights to stay online after US company withdraws domain name», *The Guardian*, 3 de diciembre de 2010, archive.today/43Jqz <<

[325] Matt Raymond, «Why the Library of Congress is Blocking WikiLeaks», *Blog de la Biblioteca del Congreso*, 3 de diciembre de 2010, archive.today/mVspZ

Ver también Ewen MacAskill, «US blocks access to WikiLeaks for federal workers», *The Guardian*, 3 de diciembre de 2010, archive.today/i1LYt

Ver también Rowan Scarborough, «Military ordered to stay off WikiLeaks», *The Washington Times*, 6 de agosto de 2010, archive.today/eZBJk <<

[326] Ewen MacAskill, «Columbia students told job prospects harmed if they access WikiLeaks cables», *The Guardian*, 5 de diciembre de 2010, archive.today/f0vgV <<

[327] Craig Labovitz, «WikiLeaks Cablegate Attack», *Blog de Abor Networks IT Security*, 29 de noviembre de 2010, archive.today/GOYuB

Ver también Craig Labovitz, «Round 2: DDoS Versus WikiLeaks», *Blog de Abor Networks IT Security*, 30 de noviembre de 2010, archive.today/CK2Mm <<

[328] Nate Anderson, «Spy games: Inside the convoluted plot to bring down WikiLeaks», *Ars Technica*, 14 de febrero de 2011, archive.today/wBM2J <<

[329] Mark Schone, Richard Esposito, Matthew Cole, Glenn Greenwald, «War on Anonymous: British Spies Attacked Hackers, Snowden Docs Show», *NBC News*, 5 de febrero de 2014, archive.today/dDR6q <<

[330] Glenn Greenwald, Ryan Gallagher, «Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters», *Intercept*, 18 de febrero de 2014, archive.today/krpPf <<

[331] «Banking Blockade», WikiLeaks, 28 de junio de 2011, archive.today/Juoc6 <<

[332] «WikiLeaks and DateCell sue Valitor for 9 billion ISK», *News of Iceland*, 5 de julio de 2013, archive.today/pWMBb <<

[333] «European Commission enabling blockade of WikiLeaks by U.S. Hardright Lieberman/King, contrary to European Parliament's wishes», WikiLeaks, 27 de noviembre de 2012, archive.today/ozC22 <<

[334] «European Parliament votes to protect WikiLeaks», WikiLeaks, 20 de noviembre de 2012, archive.today/AVjUD <<

[335] «Press Release: WikiLeaks opens path through banking siege», WikiLeaks, 18 de julio de 2012, archive.today/Yi41S

Ver también «WikiLeaks declares war on banking blockade», WikiLeaks, 16 de diciembre de 2012, archive.today/9aT0N <<

[336] «MasterCard breaks ranks in WikiLeaks blockade», WikiLeaks, 3 de julio de 2013, archive.today/boHPO <<

[337] Peter Beaumont, «WikiLeaks demands Google and Facebook unseal US subpoenas», *The Guardian*, 8 de enero de 2011, archive.today/HRGYW <<

[338] El caso se conoce oficialmente como: «Sobre el asunto de la Orden 2703(d) relacionada con las cuentas de Twitter: WikiLeaks, Rop_G, IOERROR; y BirgittaJ.» <<

[339] Julia Angwin, «Secret Orders Target Mail», *The Wall Street Journal*, 10 de octubre de 2011, archive.today/W0Sla <<

[340] Somini Sengupta, «Twitter Ordered to Yield Data in WikiLeaks Case», *The New York Times*, 10 de noviembre de 2011, archive.today/NTSQb **<<**

[341] «ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case» (comunicado de prensa), Electronic Frontier Foundation, 20 de enero de 2012, archive.today/KiVs1 <<

[342] «Government demands Twitter records of Birgitta Jonsdottir: 4th Circuit Opinion», Electronic Frontier Foundation, archive.today/3Xfpt <<

[343] Dominic Rushe, James Ball, «PRISM scandal: tech giants flatly deny allowing NSA direct access to servers», *The Guardian*, 7 de junio de 2013, archive.today/qAnuF <<

[344] Smári McCarthy, «The Dragnet at the Edge of Forever», smarimccarthy.is, 21 de junio de 2013, archive.today/CLO5x

Ver también Herbert Snorrason, «On Confirmed Assumptions, or, Not Trusting Google is Good Idea», anarchism.is, 21 de junio de 2013, archive.today/bCRkp <<

[345] Sarah Harrison, «Britain is treating journalists as terrorists — believe me, I know», *The Guardian*, 14 de marzo de 2014, archive.today/gACHR **<<**

[346] Para más información, ver «Extraditing Assange», justice4assange.com, archive.today/y3NPZ#WHAT <<

[347] «Britain’s threat to Ecuador ‘without precedent,’ says international law expert», *The Australian*, 16 de agosto de 2012, archive.today/43OD2 **<<**

[348] «Ecuador grants asylum to Julian Assange» (rueda de prensa), *WikiLeaks Press*, 16 de agosto de 2012, archive.today/oH8Au <<

Notas del traductor

[I] En el original, «Don't be evil», que es el eslogan oficial de Google y se traduce literalmente por «No seas malvado», aunque en este caso y en todos los siguientes a lo largo de libro se ha optado por «No seas malo», por la mayor semejanza entre el adjetivo «malo» y el sustantivo «mal», al que sustituye el citado eslogan en los títulos (*N. del t.*) <<

[II] Literalmente «La nueva era digital: reformando el futuro de las personas, las naciones y los negocios». Publicado en castellano por la Editorial Anaya en mayo de 2014, con el título *El futuro digital*, aunque en todas las referencias a lo largo de este libro se mantendrá el título original inglés *The New Digital Age* para evitar posibles confusiones, puesto que entre otras cosas la reseña de Assange se refiere obviamente a la versión inglesa (*N. del t.*) <<

[III] En el original, «the white geek’s burden». Alusión al poema supremacista de Rudyard Kipling *The white man’s burden* («La carga del hombre blanco»), con una vuelta de tuerca que sustituye *man* («hombre») por *geek*, término anglosajón de difícil traducción que alude a la persona poco sociable y algo excéntrica, entusiasta de los ordenadores y la informática. Aunque no posea exactamente el mismo significado, se ha optado por condensar esta definición en «friki», actualmente cada vez más empleado en castellano, hasta el punto de que la Real Academia de la Lengua Española ha decidido incluir el término en su próxima edición (*N. del t.*) <<

[IV] Expresión que denota una desgracia inminente y hace referencia al pasaje bíblico del libro de Daniel, en el cual se relata la caída de Babilonia (*N. del t.*)
<<

[V] En el inglés no existe la distinción entre trato formal (de usted) e informal (tuteo) que tiene el castellano y únicamente se puede deducir la mayor cercanía o deferencia por la situación o el tono, de ahí que en una transcripción escrita de una entrevista resulte difícil discernir en qué términos se están tratando los participantes. Sin embargo, dado el tono distendido de la grabación, y sobre todo a efectos de una mayor claridad sobre a quien se está dirigiendo cada uno de los participantes en cada momento, se ha optado por usar el tuteo en toda la traducción de la entrevista (*N. del t.*) **<<**

[VI] Susurros chinos es un juego que se juega en todo el mundo, en el que una persona susurra un mensaje a otra, que se pasa a través de una línea de gente hasta que el último jugador anuncia el mensaje a todo el grupo.

En las narraciones se suelen ir acumulando errores, por lo que la declaración anunciada por el último jugador suele diferir, normalmente de forma muy divertida, de la que pronunció el primer jugador. <<

[VII] *Graphics Interchange Format*. Lit. «Formato de Intercambio de Gráficos», GIF es un formato gráfico utilizado ampliamente en Internet tanto para imágenes como para animaciones (*N. del t.*) <<

[VIII] Juego de palabras: Jared Cohen rebautiza de forma humorística a WikiLeaks («WikiFiltraciones») por WikiForgeries («WikiFalsificaciones») (*N. del t.*) <<

[IX] La Patriot Act contra el terrorismo fue promulgada en 2001 y ha sido fuertemente criticada por organizaciones de Derechos Humanos (*N. del t.*) **<<**